Trust and e-Healthcare

Vedder, A.H.; Vantsiouri, P.; Christianen, K.

Publication date:
2012

Document Version
Publisher's PDF, also known as Version of record

Trust and e-Healthcare: a Conceptual and Legal Analysis

Report for COMMIT P15: THeCS WP 1

Tilburg Institute for Law, Technology, and Society (TILT)
Tilburg University

Mailing address
P.O. Box 90153
5000 LE Tilburg
The Netherlands

Visiting address
Montesquieu building, 7th floor
Prof. Cobbenhagenlaan 221
5037 DE Tilburg

Authors
Anton Vedder (Anton.Vedder@uvt.nl)
Patricia Vantsiouri (P.Vantsiouri@uvt.nl)
Koen Christianen (K.Christianen@uvt.nl)

October 2012

Table of Contents

Executive Summary

This report reviews the existing literature on trust in electronic services and the relevant laws and regulations with an aim to delineate the factors that can contribute to building and maintaining trust in and acceptance of electronic healthcare (e-healthcare). This report relies on academic literature and conceptual analysis in order to define trust and the concepts that affect it in a positive or a negative way. It relies on legal analysis in order to find out whether the existing legal framework can promote user trust in e-healthcare.

Defining the ethical, sociological, psychological and legal requirements for trust in e-healthcare is one of the first steps in designing trusted e-healthcare systems. On the one hand, the definition of trust can be used as a basis for designing measurable trust. On the other hand, outlining the legal context in which e-healthcare systems operate can be used as the basis for designing enforceable trust. The aim of the report is to be of help for the developers of technical standards regarding the ethical, sociological, psychological and legal requirements that they should take into consideration when designing trusted healthcare systems.

As the widespread adoption of e-healthcare is dependent both on the trust of consumers of the health services, as well as on the trust of healthcare providers, this report examines the ethical and legal requirements of trust from the perspective of the patient and of the healthcare provider.

Defining Trust

The report revisits the existing literature on trust and trust in electronic services and electronic governance in order to provide a working definition of trust, by taking into account the role that acceptance, security and privacy, transparency and reliability can play in promoting trusted e-healthcare systems. The report concludes that there is no

complete consensus as to the exact meaning of trust. However, literature generally agrees upon the following basic elements of trust:

Trust defines the relationship between a trustor, i.e., the person that trusts, and a trustee, i.e. the person or thing being trusted. Trust appears to be about expectations or beliefs in something or someone. The contents of the expectations or beliefs depend on the specifics of the particular context. Instead of explicit expectations and beliefs, trust may also have its basis in broadly shared background assumptions. Authors have also distinguished trust's dependence on either qualities of the trustee or on the trustor's disposition to trust, or on both. Often, trust is characterized as the belief that promises of or predefined expectations about other persons or entities will be fulfilled. Alternatively, trust has been defined as the willingness to adopt a vulnerable attitude towards the possibility that others do not live up to one's expectations.

Decisive ingredients of trust can relate to both the trustor and the trustee. Important elements with regard to the person or thing to be trusted are reputation, experienced performance and personal identity, i.e. a general personal character trait consisting of the general willingness to trust others.

The aforementioned requirements are crucial for building trust and acceptance in the physical off-line environment. The existing literature on e-services, though, demonstrates, that for building trust in e-healthcare it does not suffice to look at the ingredients of trust to the trustor and the trustee, but the reliability of the systems used for the provision of e-healthcare services should be also examined.

The reputation of the provider of an electronic service appears to be of utmost importance for building trust in e-healthcare services. Moreover, the ease of use of a particular website or web application appears to increase user trust. In order to promote the acceptance of e-healthcare services, users have to be aware of the availability of such electronic services. These services have to be easily accessible, easy to use, useful, compatible, trustworthy, and convenient. Advantages in terms of saving time and effort can also be important motives for trust.

The report shows that the determinants of health care professionals' acceptance of mobile healthcare systems are compatibility, perceived usefulness, and

perceived ease of use. Reliability of data, data exchange and communication is evidently important for trust in e-healthcare of caregivers. Security of databases and communications, therefore, seems to be a quintessential precondition of trust in electronic services, including e-health services.

Means for establishing reliability are also to be found in the creation of possibilities of checking for correctness and correction, e.g. by transparency and simplicity. Risks of privacy infringements are generally seen as important threats to user trust in e-health services. Indications of secure online transactions by means of technological measures such as Privacy Enhancing Technologies or authentication methods seem to increase trust of new users. Such indications enhance user trust to a greater extent than privacy policy statements, which are rarely read. Privacy by Design seems to be another promising approach towards the enhancement of the willingness to disclose data.

Furthermore, the promotion of trusted healthcare services is also contingent upon the willingness of users to provide their personal data to such systems. Users' willingness appears to increase if they trust the provider of a service, or if the user is of the opinion that the advantages of the transaction are more important than a lower level of privacy. Only by providing insight into how privacy risks are dealt with, are people able to exercise control over their data.

The Existing Legal Framework

From a legal perspective, this report considers the extent to which the law can influence trust in e-healthcare services. It concludes that although legislative intervention has followed reactively the adoption of policies to deploy e-healthcare, the law retains the power to act as a catalyst and facilitator to drive e-healthcare in the future and to build trust in such services.

Moreover, the report examines the legal framework within which trusted e-healthcare services can be offered in order to outline both the rights that e-healthcare systems and actors building and making use of such systems should respect and the responsibilities that these actors bear. In particular, it presents the norms that protect a

person's privacy as well as the existing legal rules that reinforce the reliability of healthcare providers, patients and e-healthcare systems.

As healthcare systems and the perception of healthcare differ from country to country, it is important to have national law as a starting point of reference for the legal issues that arise with regard to trusted e-healthcare services. Within the EU, healthcare is a domain that largely remains under the competence of Member States. Therefore, this report takes Dutch law as its starting point. Of course, European legal instruments are not completely missing in this field. Therefore, where relevant, EU legislation is analyzed.

Privacy, Data Protection and the Duty of Confidentiality

Privacy, or the right of an individual to be "let alone", has been recognized as a human right internationally, at a European level as well as nationally by the Dutch constitution. Two of the doctrines that safeguard a patient's right to privacy when she uses e-healthcare services are data protection law and the duty of confidentiality that healthcare professionals bear.

Data Protection

Data protection law is the doctrine that protects individuals against the illegitimate collection and processing of their personal data.The personal data that have a clear and close link with the description of the health status of a person, even administrative ones, are called health data. They fall in the category of sensitive data, which means that their processing is subject to stricter legal requirements than other personal data. In particular, although EU and Dutch data protection law does not impose an absolute ban on health data processing, it controls and channels the processing of personal data under the following strict requirements. Health data may be processed

- when the *explicit* informed consent of the data subject is obtained, *except* where the laws of a Member State provide that the prohibition may not be lifted by the data subject giving her consent.

- when the processing is necessary for the protection of the vital interests of the data subject.
- when the data are required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services.

Moreover, the person collecting and processing data should follow the general requirements set by data protection law. To elaborate, the data must be collected for specified, explicit and legitimate purposes, for example for diagnosis and treatment. To ensure the transparency of the procedure, the data processor must notify the relevant national supervisory authority about the data processing (for the Netherlands the Dutch Data Protection Authority or the appointed data protection Officer), she must provide relevant information to the data subject and she must only process the data for the purposes for which it was collected. The person in charge of collecting and processing data must ensure that the data are kept up to date while they are needed, and that they are not kept longer than necessary. Patients who provide their personal data have a right to access the data held about them, which entails to right to require information about their own personal data. Also, patients can ask for the data to be rectified, if they are incomplete or inaccurate and, under certain circumstances, patients can object the processing of their data.

The Duty of Confidentiality

The duty of confidentiality is the obligation that a healthcare provider undertakes not to disclose personal sensitive information of the patient to third parties. In the Netherlands it is regulated in the Code of Conduct for Physicians, the Healthcare Professions Act and the Dutch Criminal Code.

The duty of confidentiality entails the right and obligation of non-disclosure, which signifies that a medical practitioner has a right and an obligation to protect the patients' privacy and not disclose in front of courts or to third parties the fact that the patient committed a criminal act.

However, the duty of confidentiality is not absolute. The medical professional's oath of secrecy does not bind the professional:

- If the patient consents to the disclosure of the sensitive information;
- If information is provided to those directly involved in the provision of healthcare to the patient, provided that such disclosure is necessary;
- If data are submitted to the locum tenens, provided that it is necessary to submit these data;
- If data are presented to the patient's representative;
- If the disclosure of data is required by law;
- If data are provided on the basis of a conflict of duties;
- If disclosure of information results from a medical professional's good care.

Liability

Liability is the legal regime that determines whether a person is financially and legally responsible for something. Liability can be of civil or criminal nature. Civil liability regulates the relationship between private parties, such as patients and physicians, whereas criminal liability arises when the state punishes conduct that is not allowed by the legal order because it is held to threaten, harm or endanger interests deemed worthy. Two main sources from which civil liability may arise should be distinguished, tort and contract. Tortious liability arises from the breach of a duty primarily fixed by law; this duty is towards persons generally and its breach is redressible by an action for unliquidated damages. Contractual liability on the other hand is based upon the agreement between two parties and the assumption of responsibility by one party to the other.

In the Netherlands, a healthcare provider or a machine manufacturer can be held criminally liable for culpable homicide or serious physical injury according to the Dutch Criminal Code, whereas a patient may be held criminally liable for fraud if she tampered with the measurements of her health data.

Both will commit a tort if their action is intentional unlawful and cause damage to another person. In such a case the law dictates that the tortfeasor has the

obligation to compensate the victim for the damage that the victim suffered as a result of her intentional unlawful act. An unlawful act is intentional when it results from the tortfeasor's fault.

However, under specific strict circumstances set by the law, a person may be liable to compensate another person for damage that does not result from her fault. In particular, a person who exercises parental responsibility or legal guardianship over a child under fourteen years of age is liable for damage caused to a third person by an act of that child. Moreover, a healthcare provider may also bear liability for the tortious acts of a subordinate, such as a nurse, if she was acting in the performance of the duty assigned to her by the healthcare provider when committing the fault that caused the damage to the third party. More importantly, the EU Directive on Defective Products, which has been implemented in the Netherlands, establishes the principle of no fault-liability for damage caused by defective products, and as a result the producer, importer or supplier is held liable and must pay compensation for damage caused to persons or property resulting from a defect.

Finally, a healthcare provider, a patient or a product or network manufacturer regularly form contracts with each other and thus may be held liable to compensate the other contractual party if they failed to fulfill the obligations undertaken by contract.

Many countries apply their general liability regime in case of medical errors or negligence in providing healthcare. A number of countries, however, have introduced specific liability rules increasing protection for patients. The Netherlands belongs to the second category and has introduced specific medical liability in its Medical Treatment Agreement Act (MTAA). So, the provisions of the MTAA apply to regulate the relationship between a healthcare provider and a patient in case of for non-performance of their contract. According to the MTAA when providing medical treatment, the healthcare provider must follow the standards of a prudent healthcare provider and, in doing so, she has to act in accordance with the responsibilities laid upon her by the professional standards for healthcare providers.

Conclusions

The analysis of the role of acceptance, security, privacy, transparency, reliability and the law in building trust in e-healthcare services and the presentation of the existing legal framework demonstrate that ethics and the law can provide valuable lessons to the designers of trusted e-healthcare systems. The definition of trust and the requirements for building trust should be taken into account when designing measurable trust, whereas the legal context within which the e-healthcare systems operate can be used as a basis for designing enforceable trust.

The report also demonstrates that although there is an existing ethical, conceptual and legal framework for the provision of healthcare and the provision of electronic services, further research should be conducted in order to address the questions that the existing framework leaves unanswered with regard to e-healthcare. The next step is to advice as to alterations of the existing legal framework that will reinforce trust in e-healthcare services.

Moreover, a later report should revisit explicitly the legal issues raised here from a European and an international perspective, as the global nature of e-healthcare dictates a comparison of the legal regimes regulating e-healthcare within the EU as well as internationally. Moreover, the aim to create an open system for users and service providers that will be promoted by an international standard for trust in e-healthcare services asks for global solutions.

1 Introduction

This report reviews the existing literature on trust in electronic services and relevant laws and regulations with an aim to delineate the factors that can contribute in building and maintaining trust in and acceptance of electronic healthcare (e-healthcare). This report relies on academic literature and conceptual analysis in order to define trust and the concepts that affect it in a positive or a negative way. It relies on legal analysis in order to find out whether the existing legal framework can promote user trust in e-healthcare.

It differs from previous accounts in that it reviews the conditions of developing e-healthcare services trusted not only by patients, but also by healthcare providers. Indeed, the existing literature has focused mainly on the rights and acceptance of electronic services by patients.[1] However, incentivizing healthcare providers to develop and offer e-healthcare services is as important for the success of e-healthcare services as creating a market for such services.[2] As the widespread adoption of e-healthcare is dependent both on the trust of consumers of the health services, as well as on the trust of healthcare providers, this report examines the ethical and legal requirements of trust from the perspective of the patient and of the healthcare provider.

Defining the ethical, sociological, psychological and legal requirements for trust in e-healthcare is one of the first steps in designing trusted e-healthcare systems. On the one hand, the definition of trust can be used as a basis for designing measurable trust. On the other hand, outlining the legal context in which e-healthcare systems operate can be used as the basis for designing enforceable trust. The aim of the report is to be of help for the developers of technical standards regarding the ethical, sociological, psychological and legal requirements that they should take into consideration.

[1] Kolitsi & Iakovidis 2000; Pavlou 2003; Wilson & Lankton 2004; Carter & Bélanger 2005; Hung et al. 2009; Lee & Rao 2009; Verdegem & Verleye 2009.
[2] European Commission report 2010; Vedder 2012.

Nonetheless, defining trust is not an easy task. This is so for three reasons. First, commentators from different disciplines have adopted different definitions. Often the differences can be traced back to the specific purposes of their disciplinary backgrounds. Secondly, only some of the elements of the definitions that can be found in the extensive literature are ever-recurring, regardless of the context in which they are applied. Thirdly, the specifics of the given definitions may often depend on the different types of objects and the different types of subjects of trust particularly envisaged in a given context.

This report will build upon the common elements of the existing definitions and on specific elements that may be otherwise relevant in order to produce a working definition of user trust in e-healthcare. We do not intend to provide a conclusive, universally valid definition of trust. Our aim is rather to provide a stipulative definition that can be used for the clarification of the various elements and preconditions of user confidence in e-healthcare.

A special challenge for this report is that it is one of the first works to address the thorny issue of trust in e-healthcare. The importance of users' confidence in the responsible management and protection of health data has been highlighted in a number of studies.[3] Little work has been conducted, though, on the examination of the conditions that support trust in e-healthcare.[4] Moreover, the scope of the existing research has been confined to the support of electronic health records, whereas other aspects of the provision of e-healthcare, such as offering telemedicine services, have not attracted equal attention. Due to the lack of extensive literature on trust in e-healthcare services, this report builds mainly upon previous literature on trust in the context of electronic commerce and electronic government in order to define trust in e-healthcare.[5]

From a legal perspective, this report considers the extent to which law can influence trust in e-healthcare services. In particular, it examines the legal framework within which trusted e-healthcare services can be offered in order to outline both the

[3] Simon et al. 2009, p. 30; World Health Organization 2012.
[4] A study was conducted by the Dutch ministry on the trust of e-health records by healthcare providers. This study was confined, however, to the electronic exchange of information in a proposed national system of electronic patient records (EPD), see AMC/NIVEL 2011.
[5] Indicatively see Kool et al. 2011

rights that e-healthcare systems and actors building and making use of such systems should respect and the responsibilities that these actors bear. As healthcare systems and the perception of healthcare differ from country to country, it is important to have national law as a starting point of reference for the legal issues that arise with regard to trusted e-healthcare services. Within the EU, healthcare is a domain that largely remains under the competence of Member States.[6] Therefore, this report takes Dutch law as its starting point. Of course, European legal instruments are not completely missing in this field. Therefore, where relevant, EU legislation will be analyzed as well. Nonetheless, a later report will revisit explicitly the legal issues raised here from a European and an international perspective, as the global nature of e-healthcare dictates a comparison of the legal regimes regulating e-healthcare within the EU as well as internationally. Moreover, the aim to create an open system for users and service providers that will be promoted by an international standard for trust in e-healthcare services asks for global solutions.

In that regard Part 2 revisits the existing literature on trust and trust in electronic services in order to provide a working definition of trust, by taking into account the role that reliability, legitimacy, acceptance, accountability and privacy play in promoting trusted e-healthcare systems. Part 3 looks at the role of law in promoting trusted healthcare services and delineates the existing legal framework in the Netherlands, and, to the degree that it is relevant, at a European Union level. The report concludes that although there is an existing ethical, conceptual and legal framework for the provision of healthcare and the provision of electronic services in the Netherlands, further research should be conducted in order to address the questions that the existing framework leaves unanswered with regard to e-healthcare.

[6] Article 168 Treaty on the Functioning of the European Union.

2 Defining Trust

Trust is a key element of the relationship between caregivers and patients.[7] In e-healthcare, though, the nature and the quality of this relationship change as healthcare evolves from a series of one-to-one and face-to-face relationships to a series of parallel collaborative relationships which include remote and virtual consultations and the use of highly sophisticated and complex technological systems. There is a need, therefore, to revisit the definition of trust and to investigate how trust can be established in the context of e-healthcare services.

2.1 Trust in Traditional Contexts

There is an extensive literature on the meaning of trust in the fields of the social sciences and economics, as trust is considered to be vital for societal structures and economic systems. Nonetheless, even in these fields there is no complete consensus as to the exact meaning of trust.[8] Social scientists and economical theorists study trust as a dimension of human behavior.[9] Sociologists consider it primarily as something that facilitates the cooperation between people and enables them to build social relationships.[10]

Some examples of often cited definitions of trust are:

Deutsch 1958:

"An individual may be said to have trust in the occurrence of an event if he expects its occurrence and his expectation leads to behavior which he perceives to have greater

[7] Indicatively see Beauchamp & Childress 2001.
[8] McKnight & Chervany 1996, referring to Kee & Knox 1970, Taylor 1989, Yamagishi & Yamagishi 1994.
[9] Kool et al. 2011, p. 44.
[10] Kool et al. 2011, p. 44, referring to Buskens 1998, Doney et al. 1998, James 2002, Kipnis 1996, and Sztompka 1999.

negative motivational consequences if the expectation is not confirmed than positive motivational consequences if it is confirmed."[11]

Rotter 1967:

"[The e]xpectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon."[12]

Lewis and Weigert 1985:

"Trust exists in a social system insofar as the members of that system act according to and are secure in the expected futures constituted by the presence of each other or their symbolic representations."[13]

Mayer et al. 1998:

"The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party."[14]

Rousseau et al. 1998:

"Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another."[15]

Grandison and Sloman 2000:

"Trust is the firm belief in the competence of an entity to act dependably, securely, and reliably within a specified context."[16]

Mui et al. 2002:

"Trust is a subjective expectation an agent has about another's future behavior based on the history of their encounters."[17]

[11] Deutsch 1958, p. 266.
[12] Rotter 1967, p. 651.
[13] Lewis & Weigert 1985, p. 968.
[14] Mayer et al. 1995, p. 712.
[15] Rousseau et al. 1998, p. 395.
[16] Grandison & Sloman 2000, p. 4.

Olmedilla et al 2005:

"Trust of a party A to a party B for a service X is the measurable belief of A in that B behaves dependably for a specified period within a specified context (in relation to service X)."[18]

Nickel 2011:

"Trust is an attitude of willingness to rely on another person or entity to perform actions that benefit or protect oneself or one's interests in a given sphere of activity, together with a normative expectation: the person or entity should perform in a particular way."[19]

Although the previously mentioned definitions differ in some respects, common elements emerge as well. Trust defines the relationship between a trustor, i.e., the person that trusts, and a trustee, i.e. the person or thing being trusted.[20] If the trustee is a person, she may simultaneously act as a trustor, and *vice versa*. For example, a patient, acting as a trustor, has to be certain about the identity of the medical professional, acting as a trustee. *Vice versa*, the medical professional, who is simultaneously acting as a trustor, has to be certain about the identity of the patient, simultaneously acting as a trustee. The trustee need not always be a person, however. Animals, utensils, machines and theories can all be objects of trust as well. Both truster and trustees need not necessarily be individuals. Groups of people, professions, organizations and whole societies can be both trusters and trustees.

Trust appears to be about expectations (Deutsch; Rotter et al.; Rousseau et al.; Mui et al.) or beliefs (Grandison & Sloman; Olmedilla et al.) in something or someone. The contents of the expectations or beliefs depend on the specifics of the particular context (Deutsch; Lewis & Weigert; Mayer et al.; Grandison & Sloman;

[17] Mui et al. 2002, p. 284.
[18] Olmedilla et al. 2005, p. 195.
[19] Nickel 2011, p. 355.
[20] Taddeo 2010, p. 246.

Olmedilla et al.). Instead of explicit expectations and beliefs, trust may also have its basis in broadly shared *background assumptions* (Mui et al.). Authors have also distinguished trust's dependence on either qualities of the trustee or on the trustor's *disposition to trust*, or on both.[21] Often, trust is characterized as the belief that promises of or predefined expectations about other persons or entities will be fulfilled.[22] Alternatively, trust is defined as the willingness to adopt a vulnerable attitude towards the possibility that others do not live up to one's expectations.[23]

Decisive ingredients of trust can relate to both the trustor and the trustee. They are attributes of the trusting and the trusted person or entity, determining the level of trust and trustworthiness. An important element with regard to the person or thing to be trusted is reputation. Reputation is related to someone's or something's status, established through a stable short-term or a long-term history. Reputation often concerns the specific function or task of the person or entity involved. Another important ingredient regarding the person who trusts someone or something is *experienced performance*. Experienced performance consists of past personal experience with an individual or entity.[24] Positive past experiences of cooperation may produce trust in persons or things for the future. Experienced past performance differs from reputation, as the former is based on personal experience with a particular trustee, while the latter relates to others having had experience with a particular trustee. A third decisive factor of trust, generally agreed upon, is personal identity, a general personal character trait consisting of the general willingness to trust others.[25]

In this section we have seen that trust in its most basic meaning has to do with the expectation or belief that a person or a thing will do what it promises or can be expected to do. Generally, a personal willingness to be confident of the trustor, on the one hand, and reputation of and experienced past performance with the trustee, on the other, are considered to be important building blocks of trust.

[21] Jones 2001, p. 15918; Kool et al. 2011, p. 45; Mayer, Davis & Schoorman 1995; Das & Teng 2004; Gefen 2000; Teo & Liu 2007.
[22] Kool et al. 2011, p. 44.
[23] Doney, Cannon & Mullen 1998; Mayer, Davis & Schoorman 1995; Rosseau et al. 1998.
[24] Sztompka 1999
[25] Levi 2001; Kool et al. 2011, p. 45; Mayer, Davis, & Schoorman 1995; Das & Teng 2004; Gefen 2000; Teo & Liu 2007.

2.2 Trust in the Context of Electronic Services

Until recently, most academic studies of trust have focused on trust between persons. The introduction of electronic services has made it necessary to pay attention to the reliability of systems as well, and, even more interesting for the purposes of this study, to the reliability of systems in contexts in which reputations and past performances have not been established yet. As e-healthcare services are subspecies of electronic services, the existing literature on electronic services and trust can shed some light on the ingredients of trust in e-healthcare. They will at least clarify the features that call for extra attention in the context of electronic services. While user trust, for instance, is generally considered to be essential for commercial transactions online,[26] building user trust in e-services is deemed extra important as users may fear unwarranted access to sensitive personal information or vulnerability to identity theft or online fraud – risks that do not arise in comparable traditional off-line practices, at least not to the same degree.[27] Security of databases and communications, therefore, seems to be a quintessential precondition of trust in electronic services, including e-health services. Privacy and security issues are examined below in more detail in a special subsection.

Trust in e-services concerns both trust in the service provider, and trust in the reliability of the enabling technology.[28] This applies *mutatis mutandis* to trust in e-healthcare services, which can be subdivided into trust in the healthcare provider and trust in the reliability of the specific system used. In other words, a patient using a medical device that takes its measurements and transfers them to the physician via the internet, should not only trust the physician examining her but also the system that transfers the data. Online environments lack the benefits of the offline face-to-face communication and the possibility to directly observe the service provider's behavior. However, these problems may be tackled by technical means, such as video-chat.

[26] Buttner & Goritz 2008; Everard & Galleta 2005; Gefen 2000; McKnight, Choudhury & Kacmar 2002
[27] Colesca 2009, p. 31.
[28] Bélanger & Carter 2008, p. 166.

In academic literature trust in the internet in general is identified as a key predictor of e-service adoption.[29] This type of trust is often called institution-based trust, which refers to the individual's perception of the institutional environment, comprising the regulations and structures that make an environment safe.[30]

For users of online services experience with the use of the internet appears to be crucial for having trust in the provider of an electronic service. However, there is disagreement on whether the influence of experience with the internet is positive[31] or negative[32]. Although studies have shown that users' propensity to trust increases trust in providers of online services[33], doubts have been expressed with regard to the accuracy of those findings[34]. Other studies have shown that positive experiences with a provider of an electronic service increase the level of trust in that provider. [35] In the context of electronic services a distinction is sometimes made among the attributes of the trustee offering an online service, the attributes of the trustor and finally the attributes of the trusted electronic service (i.e. intervening technological attributes such as security and ease of use).[36] First, the reputation of the provider of an electronic service appears to be of utmost importance.[37] Reputation is particularly important for users who themselves lack experience with the provider of an electronic service.[38] Secondly, the ease of use of a particular website or web application appears to increase user trust.[39] This again seems to be especially the case with new users lacking experience with the provider of an electronic service. An inconvenient arrangement and complicated navigation appear to make the user unsure and anxious for technical mistakes.[40]

Advantages in terms of saving time and effort, can also be important motives for trust. In the context of electronic services by the government, helpfulness and

[29] Bélanger & Carter 2008, p. 167.
[30] *Ibid.*
[31] Corbitt, Thanasankit & Yi 2003
[32] Aiken & Bousch 2006; Jarvenpaa, Tractinsky & Saarinen 1999
[33] Gefen 2000; Teo & Liu 2007
[34] Koufaris & Hampton-Sosa 2004
[35] Pavlou 2003; Casalo et al. 2007; Flavian et al. 2006; Yoon 2002
[36] Kool et al. 2011, p. 45.
[37] *Ibid.*, p. 46.
[38] Chen 2006; Kim, Ferrin & Rao 2003; Koufaris & Hampton-Sosa 2004; McKnight et al. 2002
[39] Bart et al. 2005
[40] Flavian et al. 2006

simplification of complex tasks appear to increase the level of trust and user acceptance.[41]

2.3 Special Attention for Security and Privacy

Reliability of data, data exchange and communication is evidently important for trust in e-healthcare of caregivers.[42] Means for establishing reliability are of course to be found in the creation of possibilities of checking for correctness and correction, e.g. by transparency and simplicity. Other ways of establishing or protecting reliability have to do with establishing security of databases and communication. Security is also at stake where privacy is concerned. As was already mentioned, risks of privacy infringements are generally seen as important threats to user trust in e-health services.

A thorough legal analysis of privacy and data protection is provided in section 3.2.1. Here, we start out with the ethical, sociological and psychological perspectives. This subsection focuses especially on the relevance of privacy protection for user trust in e-health services. Privacy protection is aimed at safeguarding human autonomy and reducing the vulnerability of individuals, with regard to material damages, discrimination, or stigmatization.[43] Privacy also protects social values as it enables civilians to form their own opinions and preferences; it thus contributes to the diversity of ideas and fosters creativity in society.[44]

Although it is patients' privacy that should be respected and protected when e-healthcare services are offered, a lack of privacy for the patients may also affect the trust of healthcare providers in e-healthcare systems. Indeed, physicians have a professional-moral duty of confidentiality towards their patients (compare, for instance, the Hippocratic oath). As this duty is reinforced by legal obligations, healthcare providers' interests dictate that e-healthcare systems protect the privacy of their clients and that the relevant responsibilities of several other stakeholders (e.g. the

[41] Lee & Rao 2009
[42] AMC/NIVEL 2011, p. 29-32.
[43] Kool et al. 2011, p. 4.
[44] Kool et al. 2011, p. 29.

engineers who design the system and the organizations that sell (parts of) the system et cetera) are accurately and transparently divided.

Empirical research suggests that patients are concerned about the potential of electronic health information exchange to result in privacy breaches and misuse of health data.[45] The assumption that concerns about privacy affect user trust negatively lacks a firm scientific basis, however, as little empirical research has been conducted about this.[46] It has been argued that these concerns are caused by a lack of understanding of the ways in which providers of online services handle and process personal data.[47] Other researchers assume that privacy concerns are caused by the user's inability to prevent organizations from gaining access to the user's personal data.[48] The fear of users for function creep (i.e. data originally collected for one specific purpose being subsequently used for another purpose) is assumed to be another significant cause of privacy concerns.[49]

The presence of privacy policy statements on a website seems to enhance user trust.[50] However, such privacy policy statements are rarely read.[51] Indications that service providers intend to secure online transactions by means of technological measures such as Privacy Enhancing Technologies (PETs) or authentication methods seem to increase trust of new users.[52] Such indications enhance user trust to a greater extent than privacy policy statements.[53]

The willingness of users to provide their personal data appears to increase if they trust the provider of a service.[54] Secondly, the willingness to disclose personal data may increase if the user is of the opinion that the advantages of the transaction are more important than a lower level of privacy.[55]

[45] Simon et al. 2009
[46] Kool et al. 2011, referring to Hoffman et al. 1999, and Al-Awadhi & Morris 2009.
[47] Reagle & Cranor 1997
[48] Hoffman, Novak & Peralta 1999
[49] Culnan & Armstrong 1999.
[50] Lauer & Deng 2007; Meinert et al. 2004; Pan & Zinkhan 2006
[51] Arcand et al. 2007; Meinert et al. 2004
[52] Koufaris & Hampton-Sosa 2004
[53] Belanger, Hiller & Smith 2002
[54] Belanger, Hiller & Smith 2002; McKnight, Choudhury & Kacmar 2002
[55] Berendt, Gunther & Spiekermann 2005; Norberg & Dholakia 2003; Culnan & Bies 2003; Olivero & Lunt 2004

Privacy by Design (PbD) seems to be another promising approach towards the enhancement of the willingness to disclose data. PbD can be defined as the deployment of both technical and organizational safeguards during the (re)design and throughout the lifecycle of an information system (up to dismantling or replacement) in order to avoid intrusions on privacy.[56] PbD is a means of taking privacy protection into consideration (i.e. attaining privacy and data protection safeguards) at the time of the design of the processing system.[57] In the PbD approach one has to consider the necessity of the storage and processing of personal data, the means to protect personal data, solutions towards this protection, and the accompanying costs and benefits.[58] Fundamental privacy principles can be applied directly in both the design of a system and the organization. Privacy protection measures are consequently more difficult to circumvent. PbD is a more powerful and easier way of control of privacy protection than merely monitoring and enforcement of data protection legislation. Transparency is a significant element of PbD.

Only by providing insight into how privacy risks are dealt with, are people able to exercise control over their data. It is therefore essential that individuals are well-informed on how and by whom their personal data are being collected and used. They also need to know for which reasons and for how long the data are being stored. Moreover, individuals have to be informed about their rights if they want to access, remove, or rectify their data. Transparency at least includes (personal) data to be (a) easily accessible, (b) easy to understand, and (c) clearly expressed.

PbD could perhaps in part be implemented in e-healthcare applications by means of an authentication process before the healthcare provider can access the patient's personal data. Authentication can be subdivided into verification (confirming the claimed identity) and identification (determining identity). The patients' personal

[56] Kool et al. 2011, p. 33.
[57] Currently, both an unequivocal definition and agreement on the elements of Privacy by Design are lacking. The Canadian Information and Privacy Commissioner Ann Cavoukian introduced this term in the nineties of the last century subsequent to cooperation with the Dutch Data Protection Authority. They collaborated on uses of Privacy Enhancing Technologies (PETs), which is privacy protection embedded in IT-systems. The concept of Privacy by Design has subsequently been developed into a comprehensive approach. The concept is not merely about technical safeguards, but also about safeguards in business processes and a change in corporate culture.
[58] Koorn et al. 2004

data files are only accessible if the healthcare provider trying to access these records has been verified or identified. The authentication may be executed through entering a password or by means of providing biometric characteristics (such as fingerprints, iris scans, or facial images). Some personal data may for example only be accessible to the medical doctor in the hospital performing surgery, and not accessible to the psychiatrist. This type of Privacy by Design safeguards the patient's privacy.

2.4 The Start of Trust: Acceptance

An issue closely connected to the one of trust in relatively new electronic services, is the issue of the acceptance or adoption of those new services. Again extensive literature on acceptance in e-healthcare services is lacking. Nonetheless some conclusions can be derived from research on acceptance of other electronic services. It has been argued that the acceptance and use of e-government services are comparable to dynamic learning processes.[59] Dutch academic research shows that governmental policy makers often think that citizens automatically start using electronic services as soon as these are available. This, however, is not the case.[60] Unless a better alternative is presented, people will "[…] stick to the traditional non-electronic services out of habit, convenience, and lack of digital preference, access, and experience".[61] The Dutch researchers argue that the availability of e-government services should be brought to the attention of citizens to promote the acceptance and use of such services. Subsequently, so-called trigger applications can be offered to seduce citizens to use other, less popular applications.[62] The use of traditional services might be reduced as soon as people become experienced in using electronic services.[63]

Following this line of reasoning for acceptance in e-healthcare services, patients need to be seduced to use e-healthcare applications. In order to promote

[59] Van Dijk et al. 2008, p. 379.
[60] *Ibid*., p. 396.
[61] *Ibid.*
[62] *Ibid.*
[63] *Ibid.*

acceptance of e-healthcare the use of electronic services has to become customary. This can be achieved by making it more convenient. Significant predictors of citizens' intention to use e-government services are perceived ease of use, compatibility, and trustworthiness.[64] These three predictors may also be applicable to e-healthcare services. Compatibility refers to the degree to which a new technology is perceived to be consistent with the existing values, prior experiences, and needs of potential users.[65] Research shows that the determinants of health care professionals' acceptance of mobile healthcare systems are compatibility, perceived usefulness, and perceived ease of use.[66] It can be concluded that in order to promote the acceptance of e-healthcare services, users have to be aware of the availability of such electronic services. These services have to be easily accessible, easy to use, useful, compatible, trustworthy, and convenient.

2.5 Preliminary Conclusion

The analysis above demonstrates that there is no complete consensus as to the exact meaning of trust. However, literature generally agrees upon the following basic elements;

Trust defines the relationship between a trustor, i.e., the person that trusts, and a trustee, i.e. the person or thing being trusted. Trust appears to be about expectations or beliefs in something or someone. The contents of the expectations or beliefs depend on the specifics of the particular context. Instead of explicit expectations and beliefs, trust may also have its basis in broadly shared background assumptions. Authors have also distinguished trust's dependence on either qualities of the trustee or on the trustor's disposition to trust, or on both. Often, trust is characterized as the belief that promises of or predefined expectations about other persons or entities will be fulfilled. Alternatively, trust has been defined as the willingness to adopt a

[64] Carter & Bélanger 2005, p. 5.
[65] Wu et al. 2007, p. 66; Carter & Bélanger 2005, p. 8.
[66] *Ibid.* Mobile healthcare systems include mobile devices such as laptops, tablet computers, and smartphones.

vulnerable attitude towards the possibility that others do not live up to one's expectations.

Decisive ingredients of trust can relate to both the trustor and the trustee. Important elements with regard to the person or thing to be trusted are reputation, experienced performance and personal identity, a general personal character trait consisting of the general willingness to trust others.

The aforementioned requirements are crucial for building trust and acceptance in the physical off-line environment. The existing literature on e-services and e-government though, demonstrates, that for building trust in e-healthcare it does not suffice to look at the ingredients of trust to the trustor and the trustee, but the reliability of the systems used for the provision of e-healthcare services should be also examined.

The reputation of the provider of an electronic service appears to be of utmost importance for building trust in e-health services. Moreover, the ease of use of a particular website or web application appears to increase user trust. Advantages in terms of saving time and effort can also be important motives for trust.

In academic literature trust in the internet in general is identified as a key predictor of e-service adoption. Reliability of data, data exchange and communication is evidently important for trust in e-healthcare of caregivers. Security of databases and communications, therefore, seems to be a quintessential precondition of trust in electronic services, including e-health services.

Means for establishing reliability are also to be found in the creation of possibilities of checking for correctness and correction, e.g. by transparency and simplicity. Risks of privacy infringements are generally seen as important threats to user trust in e-health services. Indications of secure online transactions by means of technological measures such as Privacy Enhancing Technologies or authentication methods seem to increase trust of new users. Such indications enhance user trust to a greater extent than privacy policy statements, which are rarely read. Privacy by Design seems to be another promising approach towards the enhancement of the willingness to disclose data.

Research shows that the determinants of health care professionals' acceptance of mobile healthcare systems are compatibility, perceived usefulness, and perceived ease of use. In order to promote the acceptance of e-healthcare services, users have to be aware of the availability of such electronic services. These services have to be easily accessible, easy to use, useful, compatible, trustworthy, and convenient.

Furthermore, the promotion of trusted healthcare services is also contingent upon the willingness of users to provide their personal data to such systems. Users' willingness appears to increase if they trust the provider of a service, or if the user is of the opinion that the advantages of the transaction are more important than a lower level of privacy. Only by providing insight into how privacy risks are dealt with, are people able to exercise control over their data. It is therefore essential that individuals are *well-informed* on how and by whom their personal data are being collected and used. They also need to know for which reasons and for how long the data are being stored. Moreover, individuals have to be informed about their rights if they want to access, remove, or rectify their data. To ensure transparency the collected data should be (a) *easily accessible*, (b) *easy to understand*, and (c) *clearly expressed*.

Having viewed the definition and the requirements that can influence trust in e-healthcare, we examine whether the law can play such a role.

3 The Existing Legal Framework for the Provision of Trusted e-Healthcare Services

3.1 The Facilitative Role of Legislative Intervention in Building Trusted e-Healthcare

The question of whether and to what extent the law can influence emotional elements, like trust, and shape behaviours is not a novel one. This section aims to contribute to this controversial debate by examining whether the law can serve as a tool to promote trust in e-healthcare services.

With regard to electronic health records, a recent survey conducted by the World Health Organization suggests that law has not been successful so far in supporting the adoption of e-healthcare services.[67] The survey observes that only countries, where significant electronic health records initiatives have been adopted, have specific legislation facilitating the appropriate sharing of patient data. Moreover, significant use of e-health systems has been observed in countries with no codified legislation regulating important ethical issues, such as privacy. One such example is England, where there is no explicit reference to a legal right of privacy in common law, nor is there a codification of privacy in an English statute.[68] Nonetheless, England has made significant advances in e-healthcare through its National Health Service Connecting for Health Programme.[69]

Thus, it appears that, so far, legislative intervention has followed reactively the adoption of policies to deploy e-healthcare. This does not undermine though the power of law to act as a catalyst and facilitator to drive e-healthcare in the future and to build trust in such services. Law provides a framework in which failure to

[67] WHO survey on eHealth, p. 6, finding that legislation specifically addressing electronic health records exists predominantly in countries, where a considerable investment in eHealth has been made.
[68] This does not signify though that privacy is not protected in the UK, as people can rely on the provisions regulating breach of confidence, data protection or harassment for what is conceived as privacy violations in other countries.
[69] http://www.connectingforhealth.nhs.uk/about

implement the duties that arise from the ethical principles is addressed, it creates a realm of legal certainty in which e-healthcare may be practiced and it facilitates behaviours based on those legal principles. In other words, the role of law is to ensure that the ethical principles accepted by a community are translated into practice.

Therefore, this report examines the existing legal rules that reinforce the reliability of healthcare providers, patients and e-healthcare systems, as well as the norms that protect a person's privacy. To do so, it looks into privacy, as a human right, as well as into data protection and confidentiality issues. It looks at doctrines that protect the right to privacy, and examines the liability that healthcare providers and patients may bear when providing and using e-healthcare systems. Indeed, as e-healthcare is dependent upon the collection and sharing of patient data, it is important to examine the extent to which privacy and data protection laws and the duty of confidentiality impact upon its practice. In addition, as e-healthcare facilitates collaboration between different healthcare providers with varying levels of responsibility to the patient, this report examines whether the existing liability rules can address the issues that may arise from the provision of trusted e-healthcare services.

3.2 The Legal Framework for the Provision of e-Healthcare Services

The analysis of the legal regime regulating e-healthcare services is focused on the national law of the Netherlands, as healthcare is a domain that remains largely under the competence of Member States. The EU first gained competence in the field of public health in 1999 with the Treaty of Amsterdam.[70] However the Treaty of Lisbon, which entered into force on December 2009, amended and renumerated the public health article as Article 168 Treaty on the Function of the European Union (TFEU). Article 168 TFEU defines the role of the EU as complementing national policies, however the Union now shares competence with Member States where common safety concerns in public health are identified. Moreover, the Treaty strengthens cooperation and coordination between Member States, encourages Member States to

[70] Article 152 TEC.

establish guidelines, share best practices, set benchmarks and monitor, in order to improve the complementarity of Member States' health services in cross-border areas.[71] A major change brought by the Treaty of Lisbon is that Article 3 of the Treaty on the European Union (TEU) makes "well being" a new objective of the EU. This amendment broadens the EU's clout in e-healthcare.

Even in cases when the EU has no formal legal power to enact Union e-healthcare legislation, several other policy domains influence health policy, such as the internal market, social affairs, enterprise and economic policy. Examples of such EU legislative initiatives are the Data Protection Directive[72], the E-Commerce Directive[73], the European regulatory framework for medical devices[74] or the Directive on the transparency of measures related to the pricing and the reimbursement of medicinal products.[75]

The competence of the EU over healthcare is significant for the aims of this report to the extent that it signifies that the EU is gaining a more prominent role as an actor influencing e-healthcare. Therefore, in case a legal intervention is required to support trust in e-healthcare, it should be examined whether the Dutch government or the EU should take the relevant measures. To recommend future legislative actions, though, we must first examine the current legal framework.

[71] Article 168 TFEU.
[72] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281,23.11.1995 (Data Protection Directive).
[73] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, *OJ L 178, 17.7.2000, p. 1(*E-Commerce Directive)
[74] Directive 90/385/EEC regarding active implantable medical devices, Directive 93/42EEC regarding medical devices and Directive 98/79/EC regarding in vitro diagnostic medical devices aim at ensuring a high level of protection of human health and safety and the good functioning of the Single Market. These 3 main directives have been supplemented over time by several modifying and implementing directives, including the last technical revision brought about by Directive 2007/47/EC.
[75] Directive 89/105/EEC of 21 December 1988 relating to the transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of national health insurance systems ,*O J L 040 , 11/02/1989, p. 8-11.* The Commission published its proposal for the amendment of the transparency Directive in March 2012. See Proposal for a Directive of the European Parliament and of the Council relating to the transparency of measures regulating the prices of medicinal products for human use and their inclusion in the scope of public health insurance systems, COM(212) 84 final, 01.03.2012.

3.2.1 Privacy, Data Protection, and the Duty of Confidentiality

Privacy is the right of an individual to be "let alone" as Warren and Brandeis summarized the notion of privacy in their seminar paper in 1890.[76] It has been recognized as a human right at international, European and national level. Article 12 of the Universal Declaration of Human Rights dictates that "[n]o one shall be subjected to arbitrary interferences with his privacy" and asks for the establishment of a right "to the protection of the law against such interference or attacks". The European Convention of Human Rights stipulates in Article 8 that everyone has the right to respect for his private and family life, his home and his correspondence".[77] In the Netherlands the right to privacy was introduced by a constitutional revision in 1983. The first chapter of the Dutch Constitution codifies the right to privacy of the people of the Netherlands in Article 10. It imposes a duty on the government to protect its people against a threat to privacy posed by possible abuse of databases, a duty to regulate the right of persons to be informed about the content of such databases concerning their person and the right to correct mistakes in such content.

Two of the doctrines that safeguard a patient's right to privacy when she uses e-healthcare services are data protection law and the duty of confidentiality that healthcare professionals bear.

3.2.1.1 Data Protection

The right to privacy and the protection of personal data are not identical and do not fully overlap.[78] The aim of data protection is to control and channel the processing of personal data and not to impose an absolute ban on data processing.[79] The law protects individuals against the illegitimate collection and processing of their personal data. To achieve its aim the law provides the individual with the right to exercise

[76] Warren and Brandeis, 1890, p. 193.
[77] Article 8(1) European Convention of Human Rights. The Convention provides a jurisdiction, currently exercised by the European Court of Human Rights (ECHR) in Strasbourg, to which allegations that a Contracting State is not meeting once of its obligations can be brought.
[78] Freidewald at al, 2010.
[79] Indicatively see Article 1 Data Protection Directive.

control over her personal data, by deciding who may collect, alter, or store her data. So, data protection regulation entails provisions on consent, the right to access the data, the right to rectify, transparency enhancing provisions, the purpose limitation principle, as well as certain notification requirements.

The provision of e-healthcare services is based on the collection and processing of patients' data. Whenever an individual is examined by a physician or is tested by medical devices, a vast amount of data is collected, such as name or phone number, as well as information about the patient's health condition. The use of databases or of interconnected medical and communications devices can simplify data mining processes and create new possibilities for analyzing the data for further uses. Therefore, the analysis of the existing legal framework is indispensable.

At an international level the first initiatives to regulate data collection were taken in the 1980s by the Organisation for Economic Cooperation and Growth[80] and the Council of Europe.[81] However, as they were not successful in creating homogenous rules, the EU has enacted a number of Directives to achieve harmonisation of the processing of personal data within its territory. In particular, the Data Protection Directive[82] and the Directive on Privacy and Electronic Communications[83] have been adopted. The Data Retention Directive[84], which obliges Member States to store citizens' telecommunications data for six to twenty four months, may also apply under specific circumstances during the provision of e-health services. [85] However, data protection in the EU may change as the Commission

[80] Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, adopted on 23.09.1989.
[81] Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 108, 28.01.1981, entry into force 01.10.1985 (Data Protection Convention)
[82] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ* L 281,23.11.1995 (Data Protection Directive).
[83] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002 (as amended by Directives 2006/24/EC and 2009/136/EC)
[84] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *OJ* L105/54,13.04.2006 (Data Retention Directive),
[85] The EU has also adopted Regulation 45/2001/EC, which aims to protect personal data within EU institutions and bodies, however its provisions are unlikely to apply with regard tot eh provision of e-

proposed a major reform of the EU legal framework on the protection of personal data.[86] The current report is based on the Directives currently enforced, as the provisions of the draft General Data Protection Regulation and the draft Police and Criminal Justice Directive Data Protection Directive may change.

From the aforementioned legal instruments, the most important for the provision of trusted e-healthcare services is the Data Protection Directive. Following, the relevant provisions of the Data Protection Directive are summarized, with a focus on the provision of e-healthcare services.

a. Data Protection Directive

Purpose of the Data Protection Directive

The aim of the Directive is to protect individuals with regard to the processing of personal data, while facilitating the free movement of personal data within the EU.[87]

Types of Data that Fall Under the Scope of the Directive

The data covered by the Directive, i.e. personal data, consist of any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly by reference to an identification number or to one or more factors specific to her physical, physiological, mental economic, cultural or social identity.[88]

For example, the laboratory result of a blood sample test falls within the scope of the Directive if the identification of the originator of the blood is possible using

health services. See Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, *OJ L 8*, 12.01.2001.

[86] Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11/final, 25.0.2012 (Proposal for a General Data Protection Regulation) and Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data {SEC(2012) 72 final} {SEC(2012) 73 final}COM (2012) 10 final, 25.01.2012.

[87] Article 1 Data Protection Directive.

[88] Article 2(a) Data Protection Directive.

reasonable means. The Directive applies also if the laboratory results are stored with coded identifiers, such as a patient number. If information can be linked to a person, either by reasonably simple means, or with the help of a third person, then the data is considered identifiable. If the information refers to a group, or if it is so unique as to make it applicable to only a very small number of people, then the data could be classified as identifiable even if no actual identifier was used. For example, if the information in the file does not correspond to a name or number, but mention the disease, the profile, age, gender, postcode and profession, then the data could be classified as identifiable. [89]

Sensitive Data

Although in principle the right to privacy of the data subjects is not endangered by the content of the personal data itself, but by the context in which the processing of personal data takes place, there are specific categories of personal data that can pose threats to the right to privacy of the data subjects exactly because of their content.[90] The Data Protection Directive foresees the prohibition of processing personal data that belong to special categories, commonly known as "sensitive data". Such data are "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the *processing of data concerning health or sex life*"[91] *[emphasis added]*. Although a thorough discussion on the nature of sensitive data goes beyond the scope of this report, it should be clarified that the aforementioned categories are to be construed in a quite broad way.[92] In particular, data concerning health life (or 'health data' as they will be referred to in this report) can refer to the past, current or future physical or mental health of the data subject, as well as their drug or alcohol misuse.[93]

[89] Doosselaere et. al 2008, p. 14-15.
[90] Recital 33 Data Protection Directive; Dammann & Simitis 1997, p. 156.
[91] Article 8(1) Data Protection Directive.
[92] Kosta 2013 (forthcoming).
[93] Dammann & Simitis 1997, p 156-157.

The Article 29 Working Party introduced a broad understanding of the concept of sensitive data in relation to electronic health record systems.[94] The personal data that have a clear and close link with the description of the health status of a person are undoubtedly health data, falling in the category of sensitive data.[95] However, the Article 29 Working Party suggested a broad understanding of sensitive data in relation to data that are processed in electronic health record systems, taking the position that "all data contained in medical documentation, in electronic health records and in EHR systems should be considered as sensitive data"[96]. All data, even administrative ones, which are contained in the medical documentation of a patient, should thus be processed under the conditions of Article 8 of the Data Protection Directive, which as explained below, sets stricter requirements for the processing of sensitive data, such as health data, in comparison to the processing of other personal data. [97] The content of the categories of data identified by the Data Protection Directive as sensitive data bears an intrinsic danger against the right of the private sphere of the data subject, justifying only the exceptional processing of these data.[98]

The Duties Imposed by the Directive

Any personal data that the controller needs to process for the purposes of her professional activity must meet certain requirements. The data must be collected for specified, explicit and legitimate purposes, for example for diagnosis and treatment.[99] The processing of the data should be transparent. To ensure the transparency of the procedure, the data processor must notify the relevant national supervisory authority about the data processing, she must provide relevant information to the data subject and she must only process the data for the purposes for which it was collected. The

[94] The Article 29 Working Party is established under the Data Protection Directive, in order to give expert advice to Member States regarding data protection, to promote the harmonised application of the Directive in all Member States and to provide an opinion to the Commission on EU laws affecting the right to protection of personal data.
[95] ARTICLE 29 DATA PROTECTION WORKING PARTY, 2007, p. 7.
[96] Ibid
[97] Kosta 2013 (forthcoming).
[98] Recital 33 Data Protection Directive.
[99] Article 6 Data Protection Directive.

controller must ensure that the data is kept up to date while they are needed, and that they are not kept longer than necessary.[100]

With regard to health data, though, the Data Protection Directive prohibits in principle the processing of these data and specifies the conditions for their exceptional processing:

> *Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.*[101]

Despite the general prohibition relating to the processing of sensitive data, the Data Protection Directive foresees specific exceptions, according to which the processing of health data, is allowed. So, the Directive does not set an absolute ban on processing of health data, but a requirement that health data may be collected or processed only for certain purposes and following certain guidelines, such as the following:

- When the *explicit* informed consent of the data subject is obtained, except where the laws of a Member State provide that the prohibition may not be lifted by the data subject giving her consent.[102] Such legislation is very important to be known and respected. For example, the French Data Protection Authority (CNIL) published a recommendation on websites dedicated to health care matters pronouncing, among others, that "health care data related

[100] Article 7 Data Protection Directive.
[101] Article 8(3) Data Protection Directive.
[102] Article 2(a) Data Protection Directive.

to an identified or identifiable person may not be bought or sold, even if individuals to whom these data refer have given their consent" [103].[104]

- When the processing is necessary for the protection of the vital interests of the data subject.[105]

- When the data are required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services. In this case the data should be processed by a health professional subject under national data protection law or rules established by national competent bodies to the obligation of professional secrecy or by another also subject to an equivalent obligation of secrecy.[106]

The exceptions to the prohibition on the processing of sensitive data were actually "added in order to cover justified needs, essentially in the medical […] fields, subject to suitable safeguards", according to the position of the European Commission.[107]

The Person Who Bears Data Protection Duties

The data protection rules are addressed primarily to the data controller, i.e. the person who decides the purpose and the means of the processing.[108] That could be a senior staff member of a corporation, who is named as the person responsible for data collection and storage, or in case of small companies or self-employed individuals, the person who has legal liability for the organization. With regard to e-healthcare, the person who organizes and controls the collection of data bears the data protection duties, despite the fact that the data may be collected by a device installed in the house of the patient.

[103] CNIL 2001.
[104] Kosta 2013 (forthcoming), Kuner 2007, para. 2.98.
[105] Article 8(c) Data Protection Directive.
[106] Article 8(3) Data Protection Directive.
[107] Communication from the Commission 1995, p. 5.
[108] Article 2(c) Data Protection Directive.

Rights of the Data Subjects

Patients who provide their personal data have a right to access the data held about them, which entails to right to require information about their own personal data.[109] Also, patients can ask for the data to be rectified, if it is incomplete or inaccurate and, under certain circumstances, patients can object the processing of their data.[110] The rights of patients as data subject can reinforce the trust of patients on e-healthcare systems.

`The Data Protection Directive has been implemented in the Netherlands by the Personal Data Protection Act (*Wet bescherming persoonsgegevens*)[111]. The act was unanimously adopted by the Dutch Lower House on 23 November 1999 and accepted by the Dutch Upper House on 3 July 2000. The act came into force on 1 September 2001.

b. Personal Data Protection Act (Wet bescherming persoonsgegevens)

The Personal Data Protection Act (PDPA) applies to the fully or partly automated processing of personal data, and the non-automated processing of personal data entered in a file or intended to be entered therein[112]. The act protects personal data, such as the name, address, domicile, birth of date, health insurance company, health insurance number, health insurance policy, phone numbers, e-mail addresses, connections with other health providers, citizen service number (burgerservicenummer) of the patient. As mentioned above, such data are considered sensitive health data, when registered in Electronic Health Records.

Responsible Party

An entity that has legal authority over the processing of personal data is a "responsible party" (data controller), according to Article 1(d) PDPA. The responsible

[109] Article 12 Data Protection Directive.
[110] Article 14 Data Protection Directive.
[111] Staatsblad 2000, 302. The Staatsblad is the official journal in which all Dutch laws and most decrees are published. The Dutch Data Protection Directive entered into force on 1 September 2001.
[112] Article 2 PDPA.

party is defined as the natural person, legal person, administrative body or any other entity which, alone or in conjunction with others, determines the purpose of and means for processing personal data. The operational data processing can be conducted under the authority of the responsible party, even if the actual processing is performed by a third party, i.e. the processor. In that case an agreement has to be concluded between the responsible party and the processor.

Data Protection Authority and Data Protection Officer

The fully or partly automated processing of personal data must be notified to the Data Protection Authority (*College Bescherming Persoonsgegevens*) before the processing starts. Alternatively, businesses, branch organisations, the government and institutions can appoint their own internal supervisor of the processing of personal data, also knows as the Data Protection Officer (*Functionaris voor de Gegevensbescherming*). However, as the national supervisory authority, the Dutch DPA retains all powers with regard to organisations that have appointed a data protection officer. The appointment of the data protection officer is not common in other EU countries, but is rather a unique opportunity provided by the PDPA.

Principles for Legitimate Processing

PDPA sets a number of requirements that need to be fulfilled for data processing. Personal data must be processed in accordance with the law and in a proper and careful manner[113] and it must be collected for specific, explicitly defined and legitimate purposes[114]. The data subject should provide her consent unambiguously for the processing of her data[115] unless the processing serves the legitimate interests of the responsible party, such as savings of costs and time, avoiding errors, or improving the customer-friendly character of the services offered.[116] However, privacy concerns of the data subjects must to be considered at all times. A privacy code of conduct, which explains how to object to the collection and processing of a

[113] Article 6 PDPA.
[114] Article 7 PDPA
[115] Article 8(a) PDPA
[116] Article 8(f) PDPA

data subject's personal information, must be made available to data subjects. The data subjects' personal data may only be processed in accordance with the original purpose.[117] Data subjects' personal data collected by the healthcare provider in order to provide healthcare may be used for the administration of the healthcare practice.

Sensitive Personal Data: Data Concerning a Persons' Health

The PDPA prohibits the processing of personal data concerning a person's health (health data), unless the explicit informed consent of the subject is obtained.[118] The notion of health is interpreted broadly and it comprises all data concerning the mental and physical constitution of an individual. The prohibition on processing such personal data does not apply where the processing is carried out by medical professionals, healthcare institutions or facilities, or social services, provided that this is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned.[119] 'Administration' refers to the safeguards for the quality of provided healthcare, the processing in behalf of peer reviewing, and payments of bills.

Personal data may also be processed by other institutions, which are exhaustively listed in Article 21 PDPA. This list includes schools providing special support for pupils or making special arrangements in connection with their state of health; institutions for probation, child protection, or guardianship; the Minister of Justice; administrative bodies, pension funds, employers, or institutions working for them. For all institutions mentioned above the processing of personal data concerning a person's health must be necessary for one of the reasons stated in Article 21 PDPA. Moreover, the data concerning a person's health may only be processed by persons subject to an obligation of confidentiality by virtue of office, profession, legal provision, or contract.[120]

Personal Registration Numbers

[117] Article 9 PDPA
[118] Article 16 PDPA
[119] Article 21 PDPA
[120] Article 21(2) PDPA.

The use of personal registration numbers simplifies the connection and creates linkages among various files, although it may constitute an additional threat to private life. A variety of statutory personal registration numbers exist in the Netherlands. Pursuant to the Municipal Database Personal Records Act (*Wet gemeentelijke basisadministratie persoonsgegevens*) the Administration Number (*administratienummer*; *A-nummer*) and the Citizens Service Number (*Burgerservicenummer*; *BSN*) are issued. The Administration Number (*A-nummer*) is a personal registration number being used in the Municipal Database Personal Records (*Gemeentelijke Basisadministratie Persoonsgegevens*; *GBA*). The Administration Number and the Citizens Service Number are both being used by government agencies for the exchange of personal records.[121] From June 1st 2009 healthcare providers, health insurance companies, and care assessment agencies are obliged to use the Citizens Service Number (*BSN*). Administration numbers used internally in medical organizations and institutions do not constitute personal registration numbers according to the law. As the use of personal registration numbers may be an intrusion of one's privacy, the processing of these numbers for purposes other than the execution of law is only permitted if prescribed by law.

Privacy Code of Conduct

The PDPA permits organizations to impose stricter data protection regulations through self-regulation. Article 25 PDPA states that an organization or organizations planning to draw up a code of conduct may request the Data Protection Authority to declare that, given the particular features of the sector in which these organizations are operating, the rules contained in the proposed code of conduct are in accordance with the PDPA or other legal provisions on the processing of personal data.

[121] The present Municipal Database Personal Records (*GBA*) is being substituted by the Personal Records Database (*Basisregistratie Personen; BRP*) coming years. The Personal Records Database will provide one national registration of personal data of Dutch citizens living in the Netherlands or abroad. Keeping up to date personal data and exchange personal data is assumed to be quicker, more simply, and cheaper by means of the Personal Records Database. Not later than the year 2016 all 415 Dutch municipalities will use this new system of registration. See http://www.rijksoverheid.nl/onderwerpen/paspoort-en-identificatie/gemeentelijke-basisadministratie-gba, http://www.rijksoverheid.nl/nieuws/2012/05/07/minister-spies-geeft-startschot-voor-invoering-basisregistratie-personen.html, and http://www.programmarni.nl/onderwerpen/basisregistratie-personen.

Notification

The PDPA prescribes that the fully or partly automated processing of personal data intended to serve a single purpose or different purposes, must be notified to the Data Protection or the Data Protection officer before the processing starts (Article 27 PDPA). No notification is required for the non-automated processing of personal data intended to serve a single purpose or different related purposes. The processing of personal data is not exempted from notification in case of shared or joint responsibility.[122]

One important subsequent piece of legislation under the PDPA is the Exemption Decree (*Vrijstellingsbesluit*), which provides exemptions and simplifications to notification for certain categories of data.

Information Provided to the Data Subject

Prior to obtaining and processing personal data, the responsible party has to provide the data subject with information about its identity and the purposes of the data processing. More detailed information has to be provided in case this is necessary in order to guarantee to the data subject that the processing is carried out in a proper and careful manner.[123]

Security of Processing

The responsible party must implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. For example, a data access code restricting access to personal data may be used. Such a code may be in the form of a table indicating which medical professional has access to what personal data.[124] The so-called NEN-norm 7510 elucidates the

[122] For further information and a clarification of the regulations on the exchange of information in case of more responsible parties see http://www.cbpweb.nl/Pages/inf_va_samenwerkingsverbanden.aspx and http://www.cbpweb.nl/Pages/inf_va_melden_vrijstellen.aspx
[123] Article 33 PDPA.
[124] An example of such a table is provided by the Royal Dutch Medical Association (*Koninklijke Nederlandsche Maatschappij ter bevordering der Geneeskunst*) in their 2004 report about access to patient data in the context of the implementation of the Medical Treatment Contract Act (*Wet op de Geneeskundige Behandelingsovereenkomst*), see Witmer & De Roode 2004, p. 73.

PDPA with regard to appropriate technical measures.[125] Several other documents exist which are aimed at specific medical associations, institutions, and organizations such as general practitioners, physicians, hospitals, laboratories, and healthcare networks.

Processor Agreement

A healthcare provider may operate the automated processing of medical files herself or she may contract out this operation to a third party. The third party is the person which processes personal data for the responsible party, without having direct control over the data. In such a case, the third party is the 'processor' of personal data. The carrying out of processing by a processor must be governed by an agreement between the processor and the data controller (Article 14 PDPA).

Security Requirements

The protection of personal data has to meet particular security requirements, which are dependent on the type of data processed. Three risk categories have been created by the Dutch Data Protection Authority.[126] The basic level of risk (risk category 1) is applicable to 'regular' personal data (e.g. name and address of the data subject). The processing of personal data concerning a person's health, such as relationships between the responsible party (or processor) with healthcare providers, entails a higher level of risk (risk category 2). A higher level of risk requires higher security measures in order to fulfill the legal obligations on the protection of personal data. Personal data under medical confidentiality (risk category 3) require the highest possible security measures. According to the criteria of the Dutch Data Protection Authority concerning the processing of personal data listed in risk category 3, the responsible party is obliged to take into consideration the following aspects:

[125] This standard on information security is in April 2004 published by the Dutch Normalisation Institute (*Nederlands Normalisatie-instituut; NEN*). The revised standard had been published in 2011. The publication is titled 'Medische Informatica – Informatiebeveiliging in de zorg – Algemeen', see http://www.nen7510.org/publicaties/3507.

[126] Blarkom & Borking, 2011; College Bescherming Persoonsgegevens, Koninklijk Nederlands Instituut van Registeraccountants, and Nederlandse Orde van Register EDP-Auditors 2005.

1. Establishing security policies, security plans, and the implementation of the entire system of measures and procedures;
2. Administrative procedures of the security;
3. Promoting security awareness;
4. Requirements for recruitment and selection of staff;
5. Proper design of the workplace;
6. Management and classification of the Information and Communication Technology infrastructure;
7. Use of access controls;
8. Protection of computer networks and external connections;
9. Conditions concerning the use of third party software;
10. Security of bulk processing of personal data;
11. Requirements for storage of personal data;
12. Requirements for the destruction of personal data;
13. Preparing a disaster plan;
14. Attention to security issues regarding outsourcing of and contracts for the processing of personal data.

This implies that for the processing of personal data concerning a person's health:

- The personal data should be encrypted, if possible;
- Identification and verification measures should be in place;
- A strict authorization regime should be established. Only authorized medical professionals should have access to personal data concerning a person's health.

3.2.1.2 Duty of Confidentiality

Another expression of the right to respect the privacy of an individual is the obligation that a healthcare provider undertakes not to disclose personal sensitive information of the patient to third parties. In the Netherlands the duty of confidentiality is regulated in three instruments: a) the Code of Conduct for Physicians (*Gedragsregels voor*

artsen[127] b) the Healthcare Professions Act (*Wet beroepen in de individuele gezondheidszorg, hereinafter: HCPA*)[128] and the Dutch Criminal Code (*Wetboek van Strafrecht*, WS).

Article 88 HCPA contains a statutory duty of confidentiality for registered and unregistered practitioners. People involved in the treatment of a patient, such as medical students and secretaries, who are not licensed physicians, bear an implied duty of confidentiality.[129]

The duty of confidentiality entails the oath of secrecy and the right and obligation of non-disclosure. The intentional violation of the oath of secrecy is prosecuted based on Article 272 WS. The medical professional's right of non-disclosure is regulated in article 218 of the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, hereinafter: BWP). Pursuant to Article 160(2) BWP the person having the right of non-disclosure is not required to report a crime. The BWP recognizes in Article 165(2)(b) the right of non-disclosure to those who are bound to secrecy by virtue of their office, profession, or position. Article 68(5) of the HCPA assigns the right of non-disclosure in Article 217-219 BWP to those who are examined as witnesses or testify as experts. The right of non-disclosure has a dual nature. Firstly, it is a right of a medical professional in front of a judge. Secondly, it is an obligation that the medical professional bears in order to protect the patient's privacy. A medical professional who wrongly does not ascertains the right of non-disclosure, may bear civil, criminal or administrative liability.

For example, a doctor is bound to secrecy when she that the patient is HIV positive or has taken drugs. The same applies if a doctor made the diagnosis with a use of device that collected patient's blood at her home. The law gives priority to the duty of confidentiality instead of criminal investigation. Otherwise, access to medical treatment could be impeded. A doctor may decide to breach the duty of confidentiality

[127] Koninklijke Nederlandse Maatschappij ter bevordering der Geneeskunst (KNMG; Royal Dutch Medical Association). *Gedragsregels voor artsen (Code of conduct for physicians)*. Adopted on 25-06-2002 by the General Assembly of the federation KNMG, Article II.15.
[128] Wet van 11 november 1993, houdende regelen inzake beroepen op het gebied van de individuele gezondheidszorg (*Act of November 11th 1993 establishing rules governing the professions in individual healthcare*). *Stb.* 1993, 655.
[129] Leenen, Gevers & Legemaate 2007

if serious damage can be prevented, but only after an evaluation of the interests involved.[130]

The confidentiality is a patient's right. Therefore, the healthcare provider is not entitled to rely on her oath of secrecy in her relationship with her patients. The exception is the so called *therapeutic exception*, under which a medical professional may withhold information about a proposed medical examination or treatment of a patient if the information can cause serious harm to the patient. For example, reporting the diagnosis to a patient in an unstable mental state may lead to a suicide attempt.

The duty of confidentiality also applies to other medical professionals involved in the treatment, even though they have their own oath of secrecy. It is applicable to all information that comes to the knowledge of the medical professional, especially when it concerns facts related to the privacy of the patient entrusted to him.[131]

However, the duty of confidentiality is not absolute. The medical professional's oath of secrecy does not bind the professional in the following cases:

- If the patient consents to the disclosure of the sensitive information;
- If information is provided to those directly involved in the provision of healthcare tot the patient, provided that such disclosure is necessary;
- If data are submitted to the locum tenens, provided that it is necessary to submit these data;
- If data are presented to the patient's representative;
- If the disclosure of data is required by law;
- If data are provided on the basis of a conflict of duties;
- If disclosure of information results from a medical professional's good care.

Consent

Due to the infringing nature of sensitive data, additional safeguards should be given when the data subject gives her consent. Therefore, the *explicit* consent of the data

[130] Spiers 1995, p. 67-68; KNMG news message of September 14th 1998.
[131] See the decision of the Dutch Supreme Court, HR 23 November 1990, *NJ* 1991, 761.

subject is required, while the *unambiguous* consent that is asked for the processing of personal data in general is not deemed sufficient.[132]The patient's explicit consent can relieve the medical professional from her oath of secrecy. Explicit consent signifies that the medical professional ascertains that the patient actually assents to providing her personal data. Only those data necessary for the recipient may be provided to her by the medical professional, even if the patient has given her explicit consent.

The patient must explicitly provide her consent for a medical professional to disclose the patient's personal data:

- To another healthcare provider concerning a new medical treatment;
- To another party outside the healthcare sector (such as the police, public prosecutor, employer, lawyer, etc.);
- For academic research (unless it is not possible to ask for permission, or permission cannot reasonably be required).

Parties Directly Involved

The medical professional is not required to have permission of the patient in case she provides the patient's data to third parties directly involved in the implementation of the medical treatment agreement, such as doctors' assistants, dentist's assistants, fellow practitioners, locum tenentes (replacing doctors), nurses, nutritionists and activity coordinators.[133] However, only patient data which are necessary for these third parties may be provided to them. The necessity to provide patient data to third parties directly involved has to be weighed against the duty of confidentiality of the doctor intending to provide these data. Other medical professionals, administrators of patients' files, and employees of the finance department may also have to be consulted for the provision of the healthcare services.[134]

The group of third parties directly involved in the implementation of the medical treatment agreement can be determined bases on several criteria, which are:[135]

[132] Kosta 2013 (forthcoming)
[133] Stolker 2004 art. 7:457.
[134] Parliamentary Documents 1990-1991 p. 39; Markenstein 2006 p. 51.
[135] Dutch Data Protection Authority Report 1998.

- Is it customary in this profession to involve other medical professionals in this way with the medical treatment agreement?
- Are there reasonable alternatives?
- Does the healthcare provider have sufficient control over the actions of the third party?
- Are privacy protection measures implemented?
- Is this procedure known to the patient?
- Is this procedure in the interest of the patient?
- Is the scope of cooperation sufficiently limited?

Only those patient data necessary for the fellow medical professional to treat or diagnose the patient may be exchanged between the parties directly involved in the implementation of the medical treatment agreement.

Representative of the Patient

If the patient is not able to give her consent for legal or medical reasons, then a representative may provide consent on the patient's behalf.

Statutory Regulation

The oath of secrecy can be broken by the patient's consent or by law. An example of a legal obligation to break the oath of secrecy is the physician duty to report to the director of the municipal health service that she has suspicions that her patient has an infectious disease, as defined in Article 21 et seq of the Public Health Act (*Wet publieke gezondheid*).[136] Additionally, since the entry into force of the Health Insurance Act (*Zorgverzekeringswet*) on January 1st 2006, the healthcare providers are obliged by law to provide the health insurance companies with personal data (including medical data) about their patients in order to get reimbursement for the provided healthcare services.[137]

[136] Act of October 9th 2008 on provisions about concern for public health (*Wet publieke gezondheid*), *stb.* 2008, 460.
[137] Articles 86-93 Health Insurance Act (*Zorgverzekeringswet*).

Conflict of Duties

The oath of secrecy can also be broken when the medical professional faces a conflict of duties. In such a situation, the healthcare provider has to weigh the patient's individual interest against the public interest. In cases of child abuse, incest, sexually transmitted diseases, such as HIV infections, or if the patient has expressed the will to commit a crime, the healthcare provider bears no longer the duty of confidentiality.

In short, the medical professionals' duty of confidentiality has to be taken into account when patient data is exchanged. The duty of confidentiality applies to all information about patients, including the information that someone is a patient of a healthcare provider. Several exceptions to the duty of confidentiality exist, such as the patients' consent or the direct involvement of medical professionals in the medical treatment agreement. Preferably, permission must be obtained from the patients involved, even if such a requirement may create practical difficulties.

3.2.2 Liability

Medical practice in the age of e-healthcare is characterized by multiple physicians with multiple specialties, often in integrated delivery systems or coordinated in large institutions. Moreover, devices and software that enable the provision of e-healthcare services interfere with the diagnosis and the treatment and so do the patients, who describe their condition or take their measurements in the absence of healthcare providers. Although the good health of the patient is in the best interest of physicians, hospitals, funding bodies, machine manufacturers and of course of the patient herself, it can be anticipated that things could go wrong. The question that subsequently arises is who is legally responsible when a patient using the e-healthcare systems suffers damage.

The answer to such a question is not a simple one. When more than one person interfere with the provision of healthcare, it is harder to trace and prove which one of the aforementioned actors bears the blame for the damage caused. The situation becomes even more challenging when the damage is the result of a multitude of

factors. For example a wrong blood measurement may be caused by a malfunctioning e-health device, which could have been easily detected by the patient and should also have alarmed the physician, who could have investigated further into the matter.[138]

Secondly, as e-healthcare constitutes a new technological development, judges physicians, patients and manufacturers may not be aware of its full potential. This characteristic of e-healthcare makes the evaluation of its uses more difficult from a legal perspective. For example, the use of e-healthcare systems may be more successful in diagnosis or treatment of a number of medical conditions in comparison to traditional medical practices, however it may fail to help in the diagnosis and treatment of another medical condition, thus causing harm to the patient. In cases where the patient could have been easily diagnosed and treated if she had visited a healthcare provider in person, the legal system should define whether the patient has any rights against the physician who recommended and provided the e-healthcare service.

More importantly, imposing harsh or lenient obligations to physicians, hospitals, machine manufacturers, and patients can influence trust in e-healthcare systems in diverse ways and can create conflicting incentives for the adoption of e-healthcare services. On the one hand, the imposition of strict obligations for healthcare providers, funding bodies and machine manufacturers supports patient trust in e-healthcare. From the perspective of the patient, imposing liability to such professionals aligns their interests with that of the patient, as it makes the healthcare provider, the machine manufacturer and their funding bodies more risk averse and more cautious. On the other hand, at the early stage of the development of new technologies, such as e-healthcare systems, experimentation and taking risks may be desirable, as it can lead to advancements of the existing technological state of the art in e-healthcare.[139] Moreover, imposing liability on healthcare providers, manufacturers and funding bodies may dissuade them from providing e-healthcare services or investing in them.

[138] For further information on multiple causality in tort law see Wright, 1985.
[139] On the impact of legal standards on innovation see Salzaberger 2012.

Therefore, the law should strike a careful balance between the conflicting interests of patients and healthcare providers, so as to protect patients' health and encourage user trust in e-healthcare systems, while at the same time not dissuade the provision of e-healthcare services and investment in them. The law needs to strike a reasonable balance between the interests of the patient and the need to encourage innovation and technological development.[140]

Moreover, patients should also bear the duty to make good use of the e-healthcare systems in good faith. It is not hard to imagine scenarios where patients try to take advantage of the e-healthcare systems and the lack of the physical presence of a physician in order to defraud their insurance company, or instances when the provision of inaccurate or incomplete information or the negligent use of the e-health system can lead to damage to a patient's health. What is more challenging from a legal perspective are cases where the patient took good care of the e-healthcare system, however a third person interfered with its use without the consent or knowledge of the patient. Who should be accountable for the damage caused to the patient by a home measurement of the blood pressure of a neighbour's child, who could not have been noticed by the patient? In such cases the law needs to determine under which conditions the healthcare providers can plead the contributory fault of the claimant as a defence or in diminution of damages. The imposition of heavy obligations on patients will increase the trust of healthcare providers, funding bodies and machine manufacturers in e-healthcare services, as the risk they undertake decreases; however it could influence the trust of the patients in e-healthcare in a negative way.

The first place to look for answers to these policy questions is the existing legal regime on liability. Liability is the legal regime that determines whether a person is financially and legally responsible for something. Liability can be of civil or criminal nature. Civil liability regulates the relationship between private parties, such as patients and physicians, whereas criminal liability arises when the state punishes conduct that is not allowed by the legal order because it is held to threaten, harm or

[140] For further information with regard to Electronic Health Records see Clanahan 2008, p. 69; Rothstein 2010, p. 7.

endanger interests deemed worthy. In other words, the aim of civil liability is dispute resolution among private parties, whereas criminal liability constitutes a state intervention to protect the interests deemed worthy of protection by the legal order.

Two main sources from which civil liability may arise should be distinguished, tort and contract. Tortious liability arises from the breach of a duty primarily fixed by law; this duty is towards persons generally and its breach is redressible by an action for unliquidated damages.[141] Contractual liability on the other hand is based upon the agreement between two parties and the assumption of responsibility by one party to the other. Therefore, in tort the content of the duties is fixed by law, whereas the content of contractual duties is fixed by the contract itself. The "core" of contract is the idea of enforcing promises, whereas tort aims principally at the prevention or compensation of harms. Usually, tortious duties exist by virtue of the law itself, whereas contractual obligations are dependent upon the agreement of consent of the persons subjected to them.[142]

It should be noted that criminal liability, tortious and contractual duties may co-exist under the same facts. For example if a patient dies because of negligence of the healthcare provider, the healthcare provider may be prosecuted by the state for committing the crime of second degree murder (homicide) and may be imprisoned or made to pay a fine to the state. Moreover the healthcare provider may have not fulfilled her contractual obligation to provide medical treatment to the patient according to the standards of her profession and thus will be contractually liable to compensate the successors of the deceased patient. Finally, the healthcare provider may be found to have caused intentional damage to the relatives of the patient and thus be liable to compensate them for the emotional distress the relatives suffer because of the death of her patient.

At an EU level criminal law is not harmonised, as the Union did not have competence to legislate in that domain until the entry into force of the Treaty of Lisbon in 2009. Moreover, there are significant differences between the substantive laws of tort and contract of Member States, although some areas have been

[141] Rogers 2010, p. 6.
[142] Gerven & Larouche 2000.

harmonised within the Union.[143] For this reason the analysis of criminal, tortious and contractual liability will be focused on Dutch law.

3.2.2.1 Criminal Liability for Medical Malpractice

A healthcare provider can be held criminally liable for culpable homicide or serious physical injury according to Article 307-309 Dutch Criminal Code. If the healthcare provider commits such an offense in pursuance of her profession, she can be sentenced up to five years' and four months' imprisonment. Other possible punishments are the publication of the judgment and the temporary or permanent deprivation of her license. The healthcare provider can raise an objection, that she acted in accordance with the medical professional standard and thus her behavior should not be punished.

3.2.2.2 Tortious Liability

In the Netherlands the basis for general tortious liability lies in Article 6:162 of the Burgerlijk Wetboek (Civil Code, BW), which reads as follows:

> "*A person who commits a tortious act (unlawful act) against another person that can be attributed to him, must repair the damage that this other person has suffered as a result thereof*".

So, a successful claim for tortious liability under Article 6:162 BW must meet four cumulative requirements: Unlawfulness, Damage, Attribution and Causality.[144]

a. Unlawfulness

An unlawful act is a violation of someone else's right or entitlement or an act or omission in violation of a duty imposed by law or of what according to unwritten law

[143] Indicatively see Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, *OJ L 95*, 21/04/1993, p. 29-34.
[144] Kottenhagen & Kottenhagen-Edzes,2007, p.187.

has to be regarded as proper social conduct, as long as there was no justification for this behaviour.[145]

In the context of e-healthcare, a healthcare provider will commit a tort, if she infringes her patients' right to privacy, or if she violates her duty of confidentiality, or if her action contravenes the best practices adopted by her medical association. A patient would be tortuously liable if she infringed her insurance company's right to property by tampering the e-healthcare equipment in order to commit financial fraud.

No unlawfulness exists if the party that causes the damage has a legal excuse such as the patient's explicit consent for a medical surgery by the medical doctor.[146].

b. Damage

The unlawful behavior of the tortfeasor must result in damage to the victim. The damage may by physical, such as physical injury, financial, such as economic loss or psychological.

c. Attribution

An unlawful act can be imputed to the tortfeasor if it results from her fault or from a cause for which she is accountable according to law or common opinion.[147] In other words, the Dutch Civil Code targets both fault-based liability and strict liability. The standard for fault based liability can be either intent, or negligence. For example, a doctor who forgets that a patient is allergic to a treatment causes damage to the patient because of her fault and thus commits a tort. According to the strict liability standard a person is legally responsible for the damage caused regardless of culpability. So, if a child destroys a device used for the transmission of sensitive data, her mother will be accountable for the cause of the damage, i.e. the behavior of the child, regardless of whether she wanted, knew or could have avoided the destruction of the device. This is so because Article 6:169 BW dictates that a person who exercises parental

[145] Article 6:162(2) BW.
[146] The excuses established in Articles 40-43 Dutch Criminal Code are also applicable.
[147] Article 6:162(3) BW.

responsibility or legal guardianship over a child under fourteen years of age is liable for damage caused to a third person by an act of that child. Another example of strict liability is product liability, which is regulated in Section 6:3.3 BW. As product liability is of great significance for the provision of e-healthcare products, systems and services, it will be outlined in more detail below.

A healthcare provider may also bear liability for the tortious acts of a subordinate, such as a nurse, if she was acting in the performance of the duty assigned to her by the healthcare provider when committing the fault that caused the damage to the third party.[148] For the law to apply, the risk of the fault must have been increased by the assignment to fulfil this duty and the healthcare provider must have had control over the behaviour which constituted the fault, because of the legal relationship between her and the subordinate.

d. Causality

There must be a causal link between the damage and the unlawful act of the tortfeasor. The doctor of the previous example is liable for the damage caused by the patient's allergy to the treatment and not for damage caused the disease for which treatment was sought. The relationship between damages and act is sometimes difficult to prove as damages may be the result of causes other than the act of the healthcare provider, due to the complexity of the human body.[149]

3.2.2.3 Product Liability

A significant factor that could influence patient trust in e-healthcare is the protection afforded to patients by law from potential harm from poor goods or services in the form of imposing strict requirements of high quality. At present, no specific legislation exists at an EU or national level that specifically targets e-healthcare services and products. However, patients trusting e-healtcare are also consumers of e-

[148] Article 6:170, 171 BW.
[149] Rossendaal, 2012, p. 69.

health systems, tools and services and thus the European consumer protection regulation and its Dutch implementation could apply. The Directive on Defective Products applies to e-health products in the same way as it applies to any other product sold in the European market. Its aim is to ensure a high level of consumer protection against damage caused to health or property by a defective product. In that regard the Directive establishes the principle of no fault-liability for damage caused by defective products, and as a result the producer, importer or supplier is held liable and must pay compensation for damage caused to persons or property resulting from a defect. The injured person does not have to prove that the producer was at fault or negligent, but simply needs to prove that damage arose, that a defect in the product exists, and that there is a causal relationship between the defect and the damage.

For example, if a defective device causes an incorrect dosage to be administered, and the patient suffers harm, then the patient will not need to prove that the manufacturer of the software was aware or should have predicted that the device was defective, in order to raise a claim for compensation.

In the Netherlands the Directive on Defective products is transposed into national law in Articles 6:185-9:193 BW. According to Article 6:186 BW, a product is defective if it does not offer the safety that a person is entitled to expect, taking into account all the circumstances of the case at hand, in particular the presentation of the product, the expected use of the product, and the time the product was put into circulation.

3.2.2.4 Contractual Liability

For a person to be held liable in a contractual relationship, the Dutch Civil Code requires that she, the debtor, has failed to fulfill the obligations undertaken by the contract.[150] In addition, it is required by the law that the non-performance of the contract can be attributed to the debtor and is not due to *force majeure*.[151] A *force majeure* occurs when the debtor is not to blame for the non-performance, nor

[150] Article 6:74 BW.
[151] Article 6:75 BW.

accountable for it by virtue of law, a juridical act or generally accepted principles. The non-performance can be attributed due to fault, but also due to certain circumstances which are at debtor's risk. For example, a healthcare provider cannot be held liable for the not being able to provide care because of a power cut, that could not have been avoided. The power cut constitutes *force majeure*, an external factor that does not lie within the sphere of control of any of the contracting parties.

A further legal aspect to be examined in the framework of trusted e-healthcare is professional liability. Many countries apply their general liability regime in case of medical errors or negligence in providing healthcare. A number of countries, however, have introduced specific liability rules increasing protection for patients. The Netherlands belongs to the second category and has introduced specific medical liability in its Medical Treatment Agreement Act (MTAA) (Wet geneeskundige behandelingsovereenkomst). So, the provisions of the MTAA apply to regulate the relationship between a healthcare provider and a patient in case of for non-performance of their contract. Article 7:453 of the MTAA, which is codified in book 7 of the Dutch Civil Code, dictates that when providing medical treatment, the healthcare provider must follow the standards of a prudent healthcare provider and, in doing so, she has to act in accordance with the responsibilities laid upon her by the professional standards for healthcare providers.

The medical treatment agreement is a contract under which the healthcare provider undertakes the obligation to provide medical treatment to a patient. The healthcare provider can be a natural person, like a General Practitioner, or a legal person, such as a hospital or a online portal. The person who receives the medical treatment is 'the patient'. However, the counterparty to the contract can be a person, other than the patient. For example if a husband agrees with a doctor that the doctor will provide medical treatment to his wife, the parties to the contract are the husband and the doctor, whereas the wife is the patient.

Medical actions, as stated in Article 7:446 BW, include all activities, including examinations and providing medical consults, directly affecting a person and intended to (1) cure her, (2) to protect her from a disease, (3) to assess her state of health, (4) to provide obstetrical assistance, (5) actions other than those referred to which affect a

person directly and which are carried out by a medical doctor or dentist acting in that capacity, and (6) the attendant care and nursing of the patient and the provision for the patient's direct benefit of the material facilities under which such actions may be carried out. Such medical actions can be aimed at both bodily and mental healthcare. The MTAA is also applicable to pharmacists since 2007.

If the healthcare provides uses the assistance of auxiliary persons, such as nurses, to provide medical treatment, she is personally liable for the acts and omission of the auxiliary persons. For example, if the assistant in a General Practice centre (*huisartsenpraktijk*) enters incorrect information in an electronic patient record file in the context of the medical treatment agreement, the healthcare provider will be liable for the harm that the patient suffered because of the errors of her assistant[152]. The same holds true for liability with regard to the use of auxiliary equipment, such as computers, in the performance of an obligation. According to Article 6:77 BW if a thing is used that appears to be unfit for that purpose, the non-performance which might result from this, is attributable to the healthcare provider, unless this would be unreasonable.

The use of provisions which limit or exclude liability (*exoneratieclausules*) is quite usual in contracts. However, the MTAA in Article 7:463 explicitly prohibits the possibility to limit or exclude liability in the medical treatment agreement between the healthcare provider and the patient. Liability limitation provisions may be significant in case parties which are held liable for the patient's harm take recourse against each other. This means that the liable party that paid damages to the patient recovers these damages from the party that is to blame for the actual cause of the patient's harm. The latter party may have included liability limitation provisions in the contract, preventing the healthcare provider to recover the damages partially or entirely from the other party.

[152] Article 6:76 BW.

4 Conclusion

The aforementioned analysis of the role of reliability, legitimacy, acceptance, accountability, privacy and the law in building trust in e-healthcare services demonstrates that ethics and the law can provide valuable lessons to the designers of trusted e-healthcare systems. The definitions provided on trust and of the concepts influencing should be taken into account when designing measurable trust, whereas the legal context within which the e-healthcare systems operate can be used as a basis for designing enforceable trust.

The analysis above also demonstrates, that although there is an existing ethical, conceptual and legal framework for the provision of healthcare and the provision of electronic services, further research should be conducted in order to address the questions that the existing framework leaves unanswered with regard to e-healthcare. The next step is to advice as to alterations of the existing legal framework that will reinforce trust in e-healthcare services.

Bibliography

Aiken & Bousch 2006 K.D. Aiken & D.M. Bousch, 'Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the contextspecific nature of internet signals', *Journal of the Academy of Marketing Science* 2006, Vol. 34, pp. 308-323.

AMC/NIVEL 2011 Onderzoeksrapport afdelingen Sociale Geneeskunde & Klinische Informatiekunde AMC/NIVEL, *Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD. Een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners*, Amsterdam/Utrecht: AMC/NIVEL, 2011.

Arcand et al. 2007 M. Arcand, J. Nantel, M. Arles-Dufour & A. Vincent, 'The impact of reading a website's privacy statement on perceived control over privacy and perceived trust', *Online Information Review* 2007, Vol. 31, No. 5, pp. 661-681.

ARTICLE 29 DATA PROTECTION WORKING PARTY 2007 ARTICLE 29 DATA PROTECTION WORKING PARTY, 'Working Document on the processing of personal data relating to health in electronic health records (EHR), WP 131' (2007).

Baier 1994 A.C. Baier, *Moral prejudices: Essays on ethics*, Cambridge: Harvard University Press 1994.

Barber 1983 B. Barber, *The logic and limits of trust*, New Jersey: Rutgers University Press 1983.

Barendrecht et al. 2008 J.M. Barendrecht, M.F.M. Van Den Berg, T.F.E. Tjong Tjin Tai, and C.B.M.C. Zegveld, *Aansprakelijkheden rond het EPD*, Den Haag: Boom Juridische uitgevers 2008.

Bart et al. 2005 Y. Bart, V. Shankar, F. Sultan & G.L. Urban, 'Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study', *Journal of Marketing* 2005, Vol. 69, pp. 133-152.

Beauchamp & Childress 2001 T.L. Beauchamp & J.F. Childress, *Principles of Biomedical Ethics*, New York: Oxford University Press 2001.

Beetham 1991 D. Beetham, *The legitimation of power*, London: Macmillan 1991.

Bélanger & Carter 2008 F. Bélanger & L. Carter, 'Trust and risk in e-government adoption', *The Journal of Strategic Information Systems* 2008, Vol. 17, No. 2, pp. 165-176.

Bélanger et al. 2002 F. Bélanger, J.S. Hiller & W.J. Smith, 'Trustworthiness in electronic commerce: the role of privacy, security, and site attributes', *Journal of Strategic Information Systems* 2002, Vol. 11, pp. 245-270.

Berendt et al. 2005 B. Berendt, O. Gunther & S. Spiekermann, 'Privacy in e-commerce: stated preferences vs. actual behavior', *Communications of the ACM* 2005, Vol. 48, pp. 101-106.

Blarkom & Borking, 2011 G. W. Blarkom & J.J. Borking, *Beveiliging van persoonsgegevens*, Registratiekamer, Den Haag, april 2011, availabe at: http://www.cbpweb.nl/downloads_av/av23.pdf

Bodansky 1999 D. Bodansky, 'The Legitimacy of international governance: A coming challenge for international environmental law?' *American Journal of International Law* 1999, Vol. 93, No. 3, pp. 596-624.

Buchanan 2003 A. Buchanan, *Justice, legitimacy, and self-determination: Moral foundations for international law*, Oxford: Oxford University Press 2003.

Buskens 1998 V. Buskens, 'The social structure of trust', *Social Networks* 1998, Vol. 20, No. 3, pp. 265-289.

Buttner & Goritz 2008 O.B. Buttner & A.S. Goritz, 'Perceived trustworthiness of online shops', *Journal of Consumer Behavior* 2008, Vol. 7, pp. 35-50.

Carter & Bélanger 2005 L. Carter & F. Bélanger, 'The utilization of e-government services: citizen trust, innovation and acceptance factors', *Information Systems Journal* 2005, Vol. 15, No. 1, pp. 5-25.

Casalo et al. 2007 L.V. Casalo, C. Flavian & M. Guinaliu, 'The influence of satisfaction, perceived reputation and trust on a consumer's commitment to a website', *Journal of Marketing Communications* 2007, Vol. 13, No. 1, pp. 1-17.

Chen 2006 C. Chen, 'Identifying significant factors influencing consumer trust in an online travel site', *Information Technology and Tourism* 2006, Vol. 8, pp. 197-214.

Cheng 2003 E.K. Cheng, 'Changing scientific evidence', *Minnesota Law Review* 2003, Vol. 88, pp. 315-352.

Clanahan 2008 K. McClanahan, "Balancing Good Intentions: Protecting the Privacy of Electronic Health Information", *Bulletin of Science, Technology & Society* 28(1), 2008, p.69.

CNIL 2001 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES (CNIL), 'Délibération n° 01-011 du 08 mars 2001 portant adoption d'une recommandation sur les sites de santé destinés au publics' (2001).

Colesca 2009 S.E. Colesca, 'Increasing e-trust: a solution to minimize risk in e-government adoption', *Journal of Applied Quantitative Methods* 2009, Vol. 4, No. 1, pp. 31-44.

College Bescherming Persoonsgegevens, Koninklijk Nederlands Instituut van Registeraccountants, and Nederlandse Orde van Register EDP-Auditors 2005, College Bescherming Persoonsgegevens, Koninklijk Nederlands Instituut van Registeraccountants, and Nederlandse Orde van Register EDP-Auditors *Contouren voor Compliance. Handreiking bij het Raamwerk Privacy Audit*, 24 mei 2005, see http://www.cbpweb.nl/downloads_audit/handreiking_rpa.pdf.

Communication from the Commission 1995 Communication from the Commission to the European Parliament pursuant to the second subparagraph of Article 189 B (2) of the EC Treaty: Council common position of 20 February 1995 on the proposal for a Parliament and Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (1995) SEC(95) 303 final - COD 287, 24.02.1995, p. 5.

Corbitt et al. 2003 B.J. Corbitt, T. Thanasankit & H. Yi, 'Trust and e-commerce: A study of consumer perceptions', *Electronic Commerce Research and Applications* 2003, Vol. 2, pp. 203-215.

Culnan & Bies 2003 M.J. Culnan & R.J. Bies, 'Consumer privacy: Balancing economic and justice considerations', *Journal of Social Issues* 2003, Vol. 59, No. 2, pp. 323-342.

Dammann & Simitis 1997 U. Dammann & S. Simitis, *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft, Baden-Baden 1997.

Das & Teng 2004 T.K. Das & B.S. Teng, 'The risk-based view of trust: A conceptual framework', *Journal of Business and Psychology* 2004, Vol. 19, No. 1, pp. 85-116.

Deutsch 1958 M. Deutsch, 'Trust and suspicion', *Conflict Resolution* 1958, Vol. 2, No. 4, pp. 265-279.

Dutch Data Protection Authority Report 1998 Report of the Dutch Data Protection Authority (currently the *College Bescherming Persoonsgegevens*, formerly known as *Registratiekamer*) titled 'Medicatiebewaking door centrale patiëntenregistraties', 27 October 1998, 95.O.27.

Doney et al. 1998 P.M. Doney, J.P. Cannon & M.R. Mullen, 'Understanding the influence of national culture on the development of trust', *Academy of Management Review* 1998, Vol. 23, No. 3.

Dopselaera et al. 2008 C. van Doosselaere, J. Herveg, D. Silber & P. Wilson, "Legally eHealth, Putting eHealth in its European Legal Context", Legal and Regulatory aspects of eHealth, Study Report 2008, European Commission, Information Society and Media.

European Commission report 2010 L. Valeri, D. Giesen, P. Jansen & K. Klokgieters, *Business Models for eHealth* (Final Report prepared for ICT for Health Unit, DG Information Society and Media, European Commission, 28 February 2010), available online at: http://ec.europa.eu/information_society/activities/health/docs/studies/business_model/business_models_eHealth_report.pdf.

European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry 2011, European Coordination Committee of the Radiological, Electromedical and Healthcare IT Industry, 'COCIR Position Paper on Privacy and Health Data', 14/11/2011, available at: http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/cocir_en.pdf.

Everard & Galleta 2005 A. Everard & D.R. Galleta, 'How presentation flaws affect perceived site quality, trust, and intention purchase from an online store', *Journal of Management Information Systems* 2005, Vol. 22, No. 3, pp. 55-95.

Flavian et al. 2006 C. Flavian, M. Guinaliu & R. Gurrea, 'The role played by perceived usability, satisfaction, and consumer trust on website loyalty', *Information & Management* 2006, Vol. 43, pp. 1-14.

Franck 1988 T.M. Franck, 'Legitimacy in the international system', *American Journal of International Law* 1988, Vol. 82, No. 4, pp. 705-759.

Franck 1990 T.M. Franck, *The Power of Legitimacy Among Nations*, New York: Oxford University Press 1990.

Friedewald et al. 2010 M. Friedewald, D. Wright, S. Gutwirth & E. Mordini, 'Privacy, data protection and emerging sciences and technologies: towards a common framework', *Innovation - The European Journal of Social Science Research* 2010, Vol. 23, No. 1, pp. 61-67.

Garfinkel 1967 H. Garfinkel, *Studies in ethnomethodology*, New Jersey: Prentice-Hall 1967.

Gefen 2000 D. Gefen, 'E-commerce: The roles of familiarity and trust', *Omega* 2000, Vol. 28, pp. 725-737.

Gerven & Larouche 2000 W.Van Gerven, J. Lever & P. Larouche, Cases, Materials and Text on National, Supranational and International Tort Law, (Hart 2000).

Grandison & Sloman 2000 T. Grandison & M. Sloman, 'A survey of trust in Internet Applications', *IEEE Communications Surveys and Tutorials* 2000, Vol. 3, No. 4, pp. 2-16.

Hart 1968 H.L.A. Hart, *Punishment and Responsibility*, Oxford/New York: Oxford University Press 1968.

Held 1999 D. Held, 'The transformation of political community: Rethinking democracy in the context of globalization', pp. 84-111, in: I. Shapiro & C. Hacker-Cordón (eds.), *Democracy's Edges*, Cambridge: Cambridge University Press 1999.

Hondius 2010 E. Hondius, 'General introduction', pp. 1-26, in: E. Hondius (ed), *The development of medical liability*, Cambridge: Cambridge University Press 2010.

Hung et al. 2009 S.Y. Hung, K.Z. Tang, C.M. Chang & C.D. Ke, 'User acceptance of intergovernmental services: An example of electronic document management system', *Government Information Quarterly* 2009, Vol. 26, pp. 387-397.

Hurd 1999 I. Hurd, 'Legitimacy and authority in international politics', *International Organisation* 1999, Vol. 53, No. 2, pp. 379-408.

Hurrell 2002 A. Hurrell, ''There are no rules' (George W. Bush): International order after September 11', *International Relations* 2002, Vol. 16, pp. 185-204.

James 2002 H.S. James, 'The trust paradox: a survey of economic inquiries into the nature of trust and trustworthiness', *Journal of Economic Behavior & Organization* 2002, Vol. 47, pp. 291-307.

Jarvenpaa et al. 2002 S.L. Jarvenpaa, N. Tractinsky & L. Saarinen, 'Consumer trust in an Internet store: A cross-cultural validation', *Journal of Computer-Mediated Communication* 2002, Vol. 5, No. 2.

Jensen et al. 2005 C. Jensen, C. Potts & C. Jensen, 'Privacy practices of Internet users: self-reports versus observed behavior', *International Journal of Human-Computer Studies* 2005, Vol. 63, pp. 203-227.

Johnson-George & Swap 1982 C. Johnson-George & W.C. Swap, 'Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other', *Journal of Personality and Social Psychology*, Vol. 43, No. 6, pp. 1306-1317.

Jones 2001 K. Jones, 'Trust: Philosophical Aspects', in: *International Encyclopedia of the Social & Behavioral Sciences* 2001, pp. 15917-15922.

Kee & Knox 1970 H.W. Kee & R.E. Knox, 'Conceptual and methodological consideration in the study of trust and suspicion', *Journal of Conflict Resolution* 1970, Vol. 14, No. 3, pp. 357-366.

Kim et al. 2003 D.J. Kim, D.L. Ferrin & H.R. Rao, 'A study of the effect of consumer trust on consumer expectations and satisfaction: The Korean experience', pp. 310-315, in *Proceedings of the 5th international conference on electronic commerce*, New York: ACM.

Kipnis 1996 D. Kipnis, 'Trust and technology', pp. 39-50, in: R.M. Kramer & T.R. Tyler (eds.), *Trust in organizations: Frontiers of theory and research*, CA: Sage Publications Inc 1996.

Kolitsi & Iakovidis 2000 Z. Kolitsi & I. Iakovidis, 'Improving user acceptance of health-care telematics', *Journal of Telemedicine and Telecare*, 2000, Vol. 6, No. 2.

Koller 1988 M. Koller, 'Risk as a determinant of trust', *Basic and Applied Social Psychology* 1988, Vol. 9, No. 4, pp. 265-276.

Kool et al. 2011 L. Kool, B. van Schoonhoven, M. van Lieshout, A. Vedder & F.M. Fleurke, 'Trusted Technology: Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de electronische dienstverlening van de overheid', TNO en TILT rapport 35598 in opdracht van Alliantie Vitaal Bestuur, 2011.

Kosta 2013 E. Kosta, *Consent in European Data Protection Law*, Martinus Nijhoff – Brill (forthcoming, 2013)**.**

Kottenhagen & Kottenhagen-Edzes, 2007, R. J. P. Kottenhagen & P. A. Kottenhagen-Edzes, "Tor and Regulation Law in The Netherlands". Tort and Insurance Law Yearbook, 19(3),2007, p.187.

Koufaris & Hampton-Sosa 2004 M. Koufaris & W. Hampton-Sosa, 'The development of initial trust in an online company by new customers', *Information & Management* 2004, Vol. 41, pp. 377-397.

Kuner 2007 C. Kumer, *European data protection law - Corporate compliance and regulation*, 2nd edn Oxford University Press, Oxford 2007.

Lauer & Deng 2007 T.W. Lauer & X. Deng, 'Building online trust through privacy practices', *International Journal of Information Security* 2007, Vol. 6, pp. 323-331.

Laufer & Wolfe 1977 R.S. Laufer & M. Wolfe, 'Privacy as a concept and a social issue: A multidimensional developmental theory', *Journal of Social Issues* 1977, Vol. 33, No. 3, pp. 22-42.

Lee & Rao 2009 J. Lee & H.R. Rao, 'Task complexity and different decision criteria for online service acceptance: a comparison of two e-government compliance service domains', *Decision Support Systems* 2009, Vol. 47, pp. 424-435.

Leenen et al. 2007 H.J.J. Leenen, J.K.M. Gevers & J. Legemaate, *Handboek gezondheidsrecht. Deel 1. Rechten van mensen in de gezondheidszorg*. Houten: Bohn Stafleu Van Loghum 2007.

Levi 2001 M. Levi, 'Sociology of Trust', in: *International Encyclopedia of the Social & Behavioral Sciences* 2001, pp. 15922-15926.

Lewis & Weigert 1985 J.D. Lewis & A. Weigert, 'Trust as a Social Reality', *Social Forces*, 1985, Vol. 63, No. 4, pp. 967-985.

Lewis & Weigert 1985 J.D. Lewis & A.J. Weigert, 'Social atomism, holism, and trust', *The Sociological Quarterly* 1985, Vol. 26, No. 4, pp. 455-471.

Luhmann 1979 N. Luhmann, *Trust and power*, Chichester: John Wiley 1979.

Mayer et al. 1995 R.C. Mayer, J.H. Davis & D.F. Schoorman, 'An integrative model of organizational trust', *The academy of Management Review* 1995, Vol. 20, No. 3, pp. 709-734.

Markenstein 2006 L. Markenstein,, *Tekst en toelichting WGBO*, Editie 2006, Den Haag: Sdu uitgevers 2006, p. 51.

McKnight & Chervany 1996 D.H. McKnight & N.L. Chervany, 'The Meanings of Trust', Working Paper 1996, Carlson School of Management, University of Minnesota. Available online at: http://misrc.umn.edu/wpaper/WorkingPapers/9604.pdf.

McKnight et al. 2002 D.H. McKnight, H. Choudhoury & C. Kacmar, 'The impact of initial consumer trust on intentions to transact with a web site: A trust building model', *Journal of Strategic Information Systems* 2002, Vol. 11, pp. 297-323.

Meinert et al. 2004 D.B. Meinert, D.K. Peterson, J.R. Criswell & M.D. Crossland, 'Would regulation of website privacy policy statements increase consumer trust?', *Informing Science Journal* 2004, Vol. 9, pp. 123-142.

Merriam-Webster Online Dictionary 2012 Merriam-Webster Online Dictionary 2012, http://www.merriam-webster.com/.

Mui et al. 2002 L. Mui, M. Mohtashemi & A. Halberstadt, 'A Computational Model of Trust and Reputation', *Proceedings of the 35th International Conference on System Science* 2002, pp. 280-287.

Nickel 2011 P.J. Nickel, 'Ethics in e-trust and e-trustworthiness: the case of direct computer-patient interfaces', *Ethics and Information Technology* 2011, Vol. 13, No. 4, pp. 355-363.

Norberg & Dholakia 2004 P.A. Norberg & R.R. Dholakia, 'Customization, information provision and choice: what are we willing to give up for personal service?', *Telematics and Informatics* 2004, Vol. 21, pp. 143-155.

Olivero & Lunt 2004 N. Olivero & P. Lunt, 'Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control', *Journal of Economic Psychology* 2004, Vol. 25, pp. 243-262.

Olmedilla et al. 2005 D. Olmedilla, O.F. Rana, B. Matthews & W. Nejdl, 'Security and trust issues in semantic grids', in: 'Semantic Grid: The Convergence of Technologies', *Dagstuhl Seminar Proceedings* 2005, Vol. 05271, pp. 191-200.

Pan & Zinkhan 2006 Y. Pan & G.M. Zinkhan, 'Exploring the impact of online privacy disclosures on consumer trust', *Journal of Retailing* 2006, Vol. 82, No. 4, pp. 331-338.

Parliamentary Documents 1990-1991 Parliamentary Documents (*Kamerstukken II)*, 1990-1991, 21 561, nr. 6 (MvA).

Pavlou 2003 P.A. Pavlou, 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model', *International Journal of Electronic Commerce* 2003, Vol. 7, No. 3, pp. 101-134.

Rogers 2010, W. V. H. Rogers, *Winfield and Jolowicz on Tort,* (Sweet&Maxwell 2010), p. 6.

Roosendaal 2012 A. Roosendaal, 'Carrying Implants and Carrying Risks; Human ICT Implants and Liability', pp. 69-80, in: M.N. Gasson et al. (eds.), *Human ICT Implants: Technical, Legal and Ethical Considerations*, Information Technology and Law Series 23, The Hague: T.M.C. Asser Press 2012.

Rosenberg 1957 M. Rosenberg, *Occupations and values*, Glencoe, IL: Free Press 1957.

Rothstein 2010 M. A. Rothstein, "The Hippocratic Bargain and Health Information Technology", 38 *J.L. Med. & Ethics* 7, 2010.

Rotter 1967 J.B. Rotter, 'A new scale for the measurement of interpersonal trust', *Journal of Personality* 1967, Vol. 35, pp. 651-665.

Rotter 1971 J.B. Rotter, 'Generalized expectancies for interpersonal trust', *American Psychologist* 1971, Vol. 26, pp. 443-452.

Rousseau et al. 1998 D.M. Rousseau, S.B. Sitkin, R.S. Burt & C. Camerer, 'Not so different after al: a cross-discipline view of trust', *The Academy of Management Review* 1998, Vol. 23. No. 3, pp. 393-404.

Salzaberger 2012 E.M. Salzberger, *Law and Economics of Innovation*, (Elgar 2012).

Shapiro 1987 S.P. Shapiro, 'The social control of impersonal trust', *American Journal of Sociology* 1987, Vol. 93, No. 3, pp. 623-658.

Simon et al. 2009 S. Simon et al., 'Patients' attitudes toward electronic health information exchange: qualitative study', *Journal of Medical Internet Research* 2009, Vol. 11, No. 3.

Song et al. 2007 R. Song, L. Korba, G. Yee, *Trust in e-services: technologies, practices, and challenges*, London: Idea Group Publishing 2007.

Spiers 1995 W.J. Spiers, 'Dilemma's bij de handhaving van het medisch beroepsgeheim', in: F. de Graaf & C. Lameer (eds.), *Medisch beroepsgeheim onder druk*, Houten/Diegem: Bohn 1995.

Stolker 2004 C.J.J.M. Stolker, *Tekst & Commentaar Gezondheidsrecht, commentaar op Wet geneeskundige behandelingsovereenkomst*, Deventer: Kluwer 2004.

Sztompka 1999 P. Sztompka, *Trust: A sociological theory*, Cambridge: Cambridge University Press 1999.

Taddeo 2010 M. Taddeo, 'Modelling Trust in Artificial Agents, A First Step Toward the Analysis of e-Trust', *Minds and Machines*, 2010, Vol. 20, No. 2, pp. 243-257.

Taylor 1989 R.G. Taylor, 'The role of trust in labor-management relations', *Organization Development Journal* 1989, pp. 85-89.

Teo & Liu 2007 T.S.H. Teo & J. Liu, 'Consumer trust in e-commerce in the United States, Singapore, and China'. *Omega*, 2007, Vol. 35, pp. 22-38.

Van Dijk et al. 2008 A.G.M. van Dijk, O. Peters & W. Ebbers, 'Explaing the acceptance and use of government Internet services: A multivariate analysis of 2006 survey data in the Netherlands', *Government Information Quarterly* 2008, Vol. 25, pp. 379-399.

Vedder & Wachbroit 2003 A. Vedder & R. Wachbroit, 'Reliability of information on the internet: Some distinctions', *Ethics and Information Technology* 2003, Vol. 5, pp. 211-215.

Vedder 2008 A. Vedder, 'Responsibilities for Information on the Internet', in: K. Himma & H. Tavani (eds.), *The Handbook of Information and Computer Ethics*, New Jersey: John Wiley and Sons: 2008.

Vedder et al. 2009 A. Vedder, L. van der Wees & S. Nouwt, 'Juridische dimensies van een regionale zorggegevensadministratie', Advies Brainport Health Innovation 2009.

Vedder 2012 A. Vedder, 'Inclusive Regulation, Inclusive Design, and Technology Adoption', in: E. Palmerini and E. Stradella (eds), *Regulating Tecnological Development at the Intersection of Science and Law.* Pisa: Pisa University Press, 2012 (forthcoming).

Verdegem & Verleye 2009 P. Verdegem & G. Verleye, 'User-centered E-Government in practice: A comprehensive model for measuring user satisfaction', *Government Information Quarterly* 2009, Vol. 26, pp. 487-497.

Wang & Emurian 2005 Y.D. Wang & H.H. Emurian, 'An overview of online trust: Concepts, elements, and implications', *Computers in Human Behavior*, Vol. 21, pp. 105-125.

Warren & Brandeis, 1890 S. D. Warren & L. D. Louis, "The right to privacy", (1890) 4 *Harvard Law Review*, p. 193

Weber 1978 M. Weber, *Economy and society*, Berkeley: University of California Press 1978.

Williamson 1993 O.E. Williamson, 'Calculativeness, trust, and economic organization', *Journal of Law and Economics* 1993, Vol. 34, pp. 453-502.

Wilson & Lankton 2004 E.V. Wilson & N.K. Lankton, 'Modeling Patients' Acceptance of Provider-delivered E-health', *Journal of the American Medical Informatics Association* 2004, Vol. 11, No. 4.

Witner & De Roode 2004 J.M. Witmer & R. de Roode, 'Van wet naar praktijk. Implementatie van de WGBO. Deel 4 Toegang tot patiëntengegevens', Utrecht 2004, available online at http://knmg.artsennet.nl/Publicaties/KNMGpublicatie/Van-wet-naar-praktijk-implementatie-van-de-WGBO-Deel-2.-Informatie-en-toestemming-2004.htm.

World Health Organization 2012 World Health Organization, 'Legal Frameworks for eHealth', Based on the findings of the second global survey on eHealth', Global Observatory for eHealth series- volume 5, (WHO survey on eHealth), available at: http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf

Wright, 1985 R. W. Wright, *Causation in Tort Law*, 73 Cal. L. Rev. 1735 (1985), Available at: http://scholarship.law.berkeley.edu/californialawreview/vol73/iss6/2.

Wrightsman 1991 L.S. Wrightsman, 'Interpersonal trust and attitudes toward human nature', pp. 373-412 in: J.P. Robinson, P.R. Shaver & L.S. Wrightsman (eds.), *Measures of personality and social psychological attitudes: Vol. 1: Measures of social psychological attitudes*, San Diego: Academic Press 1991.

Yamagishi & Yamagishi 1994 T. Yamagishi & M. Yamagishi, 'Trust and commitment in the United States and Japan', *Motivation and Emotion* 1994, Vol. 18, No. 2, pp. 129-166.

Yoon 2002 S.J. Yoon, 'The antecedents and consequences of trust in online-purchase decisions', *Journal of Interactive Marketing* 2002, Vol. 16, No. 2, pp. 47-63.